ZAPOBIEGANIE: OBRONA TECHNICZNA

* Ochrona fizycznej infrastruktury informatycznej. Zabezpieczenia obiektów i zarządzanie kryzysowe

* Bezpieczeństwo systemu operacyjnego. Podstawy bezpieczeństwa systemów operacyjnych, w tym jądra bezpieczeństwa, poziomy uprawnień, listy kontroli dostępu i partycje pamięci

* Sieci lokalne. Bezpieczeństwo sieci lokalnych, w tym zasady i narzędzia specyficzne dla platformy

* Urządzenia zabezpieczające bramę. Skuteczne zalecenia dotyczące wdrażania zapór i serwerów proxy

* Urządzenia do wykrywania włamań i zapobiegania włamaniom. Krytyczne elementy zarządzania bezpieczeństwem w celu pomiaru częstotliwości ataków na zewnątrz i wewnątrz obwodu oraz w celu ograniczenia skutecznej penetracji

* Identyfikacja i uwierzytelnianie. Co wiemy, co mamy, czym to jest i co robi

* Uwierzytelnianie biometryczne. Szczególny nacisk kładziony jest na to, kim się jest i co robi jako wyznaczniki tożsamości

*Zabezpieczenia handlu elektronicznego i serwera WWW. Środki technologiczne i prawne leżące u podstaw bezpiecznego handlu elektronicznego oraz systematyczne podejście do opracowywania i wdrażania usług bezpieczeństwa

*Monitorowanie sieci i filtrowanie treści. Narzędzia do zarządzania bezpieczeństwem na obwodzie

* Wirtualne sieci prywatne i bezpieczny dostęp zdalny. Szyfrowane kanały (wirtualne sieci prywatne) dla bezpiecznej komunikacji i podejścia do bezpiecznego zdalnego dostępu

* Bezpieczeństwo bezprzewodowej sieci LAN 802.11. Ochrona coraz bardziej rozpowszechnionych sieci bezprzewodowych, ponieważ większość użytkowników Internetu na świecie uzyskuje dostęp do informacji za pośrednictwem swoich telefonów komórkowych i tabletów

* Zabezpieczanie VoIP. Środki bezpieczeństwa dla telefonii Voice over IP, opłacalnej metody zwiększania współpracy na odległość

* Zabezpieczanie narzędzi P2P, IM, SMS i narzędzi współpracy. Zabezpieczanie narzędzi do współpracy, takich jak sieci peer-to-peer, wiadomości błyskawiczne, usługi wysyłania wiadomości tekstowych i inne mechanizmy ograniczające fizyczne podróże oraz ułatwiające komunikację

* Zabezpieczanie przechowywanych danych. Zarządzanie szyfrowaniem i wydajne przechowywanie przechowywanych danych, w tym usług przechowywania w chmurze

* PKI i urzędy certyfikacji. Pojęcia, terminologia i zastosowania infrastruktury klucza publicznego do szyfrowania asymetrycznego

* Pisanie bezpiecznego kodu. Wskazówki dotyczące pisania solidnego kodu programu, który zawiera kilka błędów i który może skutecznie przeciwdziałać celowym atakom

* Rozwój oprogramowania i zapewnianie jakości. Korzystanie z zapewniania jakości i testowania w celu wzmocnienia bezpieczeństwa na etapie opracowywania programów

* Zarządzanie łatkami i lukami w oprogramowaniu. Racjonalne wdrażanie poprawek oprogramowania

* Technologia antywirusowa. Metody walki ze złośliwym kodem

* Ochrona praw cyfrowych: podejścia techniczne. Metody ochrony własności intelektualnej, takie jak programy, muzyka i wideo, które ze swej natury muszą być udostępniane, aby były użyteczne

WPROWADZENIE.

Wcześniejsze wpisy opisywały systematyczne podejście do identyfikacji zagrożeń dla fizycznej infrastruktury informacyjnej. Od tego momentu będziemy opisywać praktyczne zalecenia dotyczące wdrażania dobrej ochrony bezpieczeństwa fizycznego systemów informatycznych (IS). Był czas, kiedy ubezpieczenie wystarczyło na pokrycie większości sytuacji zagrożenia. Jednak dziś ubezpieczenie od klęsk żywiołowych, przemocy w miejscu pracy i ubezpieczenia od terroryzmu mogą być niedostępne lub niedrogie bez niezależnego zewnętrznego audytu bezpieczeństwa w celu ustalenia, czy istnieje dobry program bezpieczeństwa. Istnieje jedna prawie żelazna obrona prawna przed zarzutami zaniedbań, a to ma na celu wykazanie, że organizacja przestrzega powszechnie przyjętych procedur planowania i zarządzania bezpieczeństwem. Zwykle sama zgodność jest wystarczająca, aby nawet wnieść pozew o zaniedbanie; wszelkie pozostałe zarzuty są zwykle niewielkie i można je łatwo objąć ubezpieczeniem. Zgodność z powszechnie akceptowanymi procedurami można szybko ustalić podczas ostatniego audytu bezpieczeństwa. Audyt bezpieczeństwa zbada zgodność ze wszystkimi udokumentowanymi aspektami planowania, przygotowania, polityk, szkoleń i ćwiczeń, zarządzania i nadzoru oraz planów i procedur reagowania i odzyskiwania. Są to wszystkie niezbędne elementy do ochrony infrastruktury informacyjnej.

PLANOWANIE I ZARZĄDZANIE BEZPIECZEŃSTWEM

W Stanach Zjednoczonych istnieje wiele przepisów ustawowych, wykonawczych i federalnych, które należy włączyć do planowania bezpieczeństwa i zarządzania każdą organizacją. Nawet jeśli zgodność nie jest jeszcze obowiązkowa, zdecydowanie zaleca się po prostu uniknięcie niepotrzebnych i potencjalnie ogromnych kosztów obrony przed zarzutami zaniedbania i ustalenia w sądzie, że obowiązujące procedury bezpieczeństwa są wystarczające. Niektóre nowe wymagania, które mogą mieć wpływ na prawie każdą organizację w Stanach Zjednoczonych, zostały krótko streszczone na poniższej liście.

Zgodność z krajowym systemem zarządzania incydentami (NIMS): Krajowy system zarządzania incydentami (NIMS) zdefiniowany przez FEMA wymaga od wszystkich departamentów i agencji władz federalnych, stanowych i lokalnych wdrażania jej standardów. NIMS to szablon reagowania kryzysowego, który uzupełnia i ujednolica systemy dowodzenia incydentami od dawna używane przez większość agencji reagowania.

Krajowe ramy reagowania: Krajowe ramy reagowania (NRF) stanowią plan operacji kryzysowych, który od dawna wymaga się od wszystkich władz stanowych i lokalnych. NRF ujednolica teraz treść i format wszystkich takich planów. Zgodność wymaga również certyfikacji wyższych urzędników.

Krajowy plan ochrony infrastruktury: Krajowy plan ochrony infrastruktury (NIPP) określa zalecenia dotyczące ochrony infrastruktury krytycznej i kluczowych zasobów. Proponuje ujednoliconą strukturę obejmującą inicjatywy partnerskie, ramy zarządzania ryzykiem i wymianę informacji.

Robert T. Stafford Ustawa o pomocy humanitarnej w sytuacjach kryzysowych i pomocy w sytuacjach kryzysowych z 1988 r. (PublicLaw 100-707): W połączeniu z Ustawą o łagodzeniu skutków katastrof z 2000 r. (Ustawa publiczna 106-390), każde państwo i społeczność musi mieć aktualne i zatwierdzone przez FEMA All- Plan ograniczenia zagrożeń oraz obowiązujący i zatwierdzony plan działań awaryjnych.

Ustawa Sarbanes-Oxley z 2002 r. (SOX): Korporacje publiczne muszą zgłaszać wszystkie swoje wewnętrzne kontrole finansowe, w tym te związane z zarządzaniem bezpieczeństwem - w tym przyszłe zdarzenia, które mogą mieć istotny wpływ na przyszłe zarobki.

Ustawa o przenośności i rozliczalności ubezpieczeń zdrowotnych z 2002 r. (HIPAA): Wszystkie organizacje, które otrzymują i przechowują dane osobowe, muszą identyfikować te dane.

Ustawa Gramm-Leach-Bliley z 1999 r .: instytucje finansowe, pożyczkodawcy, doradcy, księgowi i firmy przetwarzające lub otrzymujące informacje finansowe muszą chronić te dane przed nieuprawnionym ujawnieniem i modyfikacją.

Program akredytacji zarządzania kryzysowego (EMAP): EMAP, „niezależna organizacja non-profit, jest opartym na standardach dobrowolnym procesem akredytacji oceny i wzajemnej oceny programów rządowych odpowiedzialnych za koordynację działań prewencyjnych, łagodzących, gotowych, reagujących i przywracania zdrowia naturalnego i ludzi spowodował katastrofy. Akredytacja opiera się na zgodności ze wspólnie opracowanymi standardami krajowymi, czyli Standardem Zarządzania Kryzysowego EMAP. Akredytacja jest dostępna dla wszystkich stanów USA, terytoriów i lokalnych programów zarządzania kryzysowego. Każdy może subskrybować, aby otrzymywać standardy i materiały informacyjne

STRATEGICZNY PROCES PLANOWANIA.

Proces planowania musi myśleć strategicznie z wyprzedzeniem, aby określić najlepsze możliwe opcje bezpieczeństwa, aby dodać maksymalną wartość i przyczynić się do zysków, zwiększyć wydajność i wydajność oraz uniknąć ingerencji. Proces identyfikowania wszystkich możliwych sytuacji zagrożenia oraz metodę statystyczną służącą do przewidywania prawdopodobieństwa obrażeń lub szkód oraz bieżącej podatności przedsiębiorstwa na poszczególne zagrożenia opisano wcześniej. Tu opieramy się na procesie planowania, sugerujemy sposoby lepszej ochrony infrastruktury, a tym samym zmniejszenia jej podatności na zagrożenia, oraz opisuje, jak wdrożyć proces planowania i zarządzania bezpieczeństwem. Niektóre aspekty dobrej ochrony fizycznej, które należy wziąć pod uwagę w procesie planowania, zostały przedstawione w dalszej części. Sugerują one pewne krytyczne elementy i sposoby ich ochrony, a także niektóre możliwe słabe punkty infrastruktury informacyjnej.

Atrakcyjne cele.

Znaczna część wpisów dotyczy tego, co oznacza fizyczne hakowanie. Podobnie jak w przypadku jego elektronicznego odpowiednika, fizycznych ataków nie można przewidzieć kiedy, gdzie i jak będą się pojawiać. Hakowanie elektroniczne w organizacji, za pośrednictwem jej sieci lub z dowolnego miejsca na świecie za pośrednictwem Internetu jest nadal najlepszym sposobem włamania się do większości systemów informatycznych. Jednak fizyczna ingerencja może być trudniejsza do wykrycia i zlokalizowania, a często jest bardziej szkodliwa i kosztowna. Ponadto poważnym zagrożeniem są zagrożenia ze strony pracowników lub kontrahentów, którzy są złymi aktorami posiadającymi upoważnienie do nadzoru bez nadzoru w pracy z fizyczną infrastrukturą systemów informatycznych lub w ich pobliżu.

Strategie obronne.

Należy rozważyć wiele skutecznych strategii obronnych. Proces planowania musi oceniać każde podejście i jak najlepiej połączyć je strategicznie, aby zmaksymalizować skuteczność i zminimalizować koszty. Te strategie obronne są powszechne:

* Zapobieganie, aby określone zagrożenia nie wpływały na przedsiębiorstwo.

* Odstraszanie, aby nie wystąpiły określone zagrożenia.

* Łagodzenie w celu zmniejszenia każdego zagrożenia do dopuszczalnych konsekwencji.

* Redundancje, więc nie ma krytycznych łączy w infrastrukturze, których nie można obejść. Istnieje wiele metod redundancji, takich jak wiele ścieżek danych; dwukierunkowe pętle danych; przetwarzanie równoległe lub rozproszone; alternatywne systemy wsparcia i narzędzia; i wiele więcej.

* Wczesne ostrzeżenie w celu wykrycia zbliżającego się problemu i opóźnienia, aby szybka reakcja mogła zapobiec zakłóceniom lub zminimalizować je.

* Warstwy bezpieczeństwa, które są jak koncentryczne warstwy cebuli, tak że kilka warstw bezpieczeństwa musi zostać przebite, zanim cel zostanie osiągnięty. Zwiększa to niezawodność, ponieważ uszkodzenie lub naruszenie jednej warstwy nie zagraża innym koncentrycznym warstwom.

* Ubezpieczenie, które może zwrócić część kosztów odzyskiwania, ale zwykle niewiele kosztów reakcji. Ochrona ubezpieczeniowa często wyklucza wiele zagrożeń i może być kosztowna. Ubezpieczenie może nie obejmować (a nawet być dostępne) rażącego zaniedbania, niektórych działań Boga, powodzi, terroryzmu lub działań wojennych.

* Rynki kapitałowe, które są mniej kosztowne niż ubezpieczenie i lepiej potrafią odłożyć większe i szersze ryzyko.

* Samoubezpieczenie w celu ustalenia retencji (które są środkami zgromadzonymi w tym celu) w nadziei, że nic poważnego się nigdy nie wydarzy.

* Usługi ochrony kontraktów wykonywane są wewnętrznie, które zasadniczo przenoszą ryzyko, ale niekoniecznie ograniczają zagrożenia.

* Outsourcing, który jest kolejną opcją, która wprowadza jeszcze inne i często niezrealizowane zagrożenia i luki.

Kto jest odpowiedzialny?

Skuteczne bezpieczeństwo wymaga zarówno zarządzania ze strony zarządu, jak i nadzoru ze strony kierownictwa wyższego szczebla. Najwyższe kierownictwo musi również aktywnie sponsorować to i nalegać, aby wszyscy zaangażowani rozumieli, wspierali i szanowali plany i procedury bezpieczeństwa. Niezbędna jest odpowiedzialność i nadzór, podobnie jak naleganie na okresowe ćwiczenia bezpieczeństwa, przegląd i aktualizację. Jeśli to możliwe, menedżer ds. bezpieczeństwa infrastruktury nie powinien również odpowiadać za IS, bezpieczeństwo korporacyjne lub lokalowe. Chociaż menedżerowie tych obszarów stają w obliczu podobnych zagrożeń, a ich grupy muszą ściśle ze sobą współpracować, ich priorytety i poziomy reakcji na każdy incydent są różne. Dlatego najlepiej, aby dwie lub więcej wyspecjalizowanych grup bezpieczeństwa podlegało jednemu z wyższych rangą dyrektorów wykonawczych posiadających jasne uprawnienia. Nawet jeśli rola nie może być pełnoetatowa, określenie formalnej pozycji dla bezpieczeństwa infrastruktury menedżer to mądra inwestycja.

Jeden proces, jeden język.

Jak wspomniano wcześniej, proces planowania i zarządzania bezpieczeństwem musi być jednolity i wszechstronny oraz stosowany skutecznie i wydajnie. Powinien również zostać przeprowadzony bieżący audyt przeprowadzany przez zewnętrzną, niezależną grupę w celu upewnienia się zarówno o gotowości bezpieczeństwa, jak i zgodności z odpowiednimi przepisami prawa, kodeksami i regulacjami. Najmniej kosztownym i najskuteczniejszym podejściem jest przestrzeganie federalnych wytycznych. Procedury Departament Bezpieczeństwa Wewnętrznego (DHS) i FEMA zapewniają jednolitą i

wszechstronną metodologię oraz ogólnie przyjęte standardowe praktyki, które są jednolite, wszechstronne i mogą również odstraszać od odpowiedzialności. Ten proces jest zalecany dla każdej organizacji, publicznej lub prywatnej. FEMA rozróżnia sytuację awaryjną, czyli sytuację, w której organizacja może poradzić sobie z własnymi zasobami i katastrofą, która ma miejsce, gdy zasoby wewnętrzne mogą zostać przeciążone i potrzebna jest pomoc z zewnątrz. To rozróżnienie nie zawsze jest wyraźne. „Kryzys" nie jest terminem zdefiniowanym. FEMA zaleca również planowanie i przygotowanie na gorsze sytuacje, które często okazują się tym, co się dzieje. Wiele zagrożeń może stać się katastrofą dla firmy, nawet jeśli zasoby zewnętrzne reagują szybko. Na przykład konsekwencje pożaru w pomieszczeniu z wyposażeniem mogą być katastrofalne, gdy lokalna straż pożarna reaguje siekierami i wężami wodnymi, odcina całą energię elektryczną w budynku i wybija okna, aby odprowadzić dym. Nawet poważny incydent, który ma miejsce z dala od bezpośredniej siedziby, może wymagać ewakuacji, odcięcia zasilania budynku i spowodowania poważnych zakłóceń.

ELEMENTY DOBREJ OCHRONY.

Ochrona infrastruktury na ogół wymaga innych i silniejszych zabezpieczeń niż mogą zapewnić zabezpieczenia lokali lub logiczne zabezpieczenia IS. Ochrona infrastruktury musi być skuteczna, wydajna i niedroga. Jednak musi być również nieinwazyjny i przyjazny dla użytkownika. Zbyt duża ochrona jest niepotrzebnie kosztowna i często przynosi efekt przeciwny do zamierzonego. Zbyt mało może być jeszcze bardziej kosztowne i zagrozić produktywności, morale i dobrej woli. W następnych sekcjach przedstawiono niektóre elementy niezbędne do zapewnienia odpowiedniego poziomu ochrony.

Segmentowane sekrety

Chociaż bezpieczeństwo przez zaciemnienie jest słusznie wyśmiewane, jeśli jest głównym celem ochrony, aby utrzymać dobre bezpieczeństwo, nikt nie powinien znać ani kontrolować wszystkich szczegółów lub pracy wewnętrznej systemów i procedur bezpieczeństwa. Jeśli całkowite zrozumienie systemów bezpieczeństwa zostanie podzielone na kilka części, a wiedza zostanie rozprowadzona między współpracownikami, istnieje znacznie mniejsze prawdopodobieństwo nadużycia, oszustwa lub błędu i mniejsze uzależnienie od kilku kluczowych osób. Wspólna wiedza przyczynia się do rozdzielenia obowiązków i wszechobecnej czujności. Jednak im więcej osób zna systemy i procedury bezpieczeństwa, tym bardziej systemy te stają się podatne na ataki. Łatwiej jest zagrozić bezpieczeństwu poprzez przymus lub wymuszenie lub przez nierozsądne uwagi nieumyślne ujawnienie informacji. Lista osób posiadających wiedzę wewnętrzną może obejmować menedżerów, administratorów, personel konserwacyjny, użytkowników, partnerów, dostawców, klientów, sprzedawców i konsultantów. Chociaż wiele osób musi znać przynajmniej niektóre zabezpieczenia, nikt nie musi znać wszystkich szczegółów. Oprócz segmentacji konieczne jest inne zabezpieczenie, które zapewni dobrą ochronę. Jeśli członkowie tej samej grupy muszą dzielić się wrażliwą wiedzą, powinna obowiązywać zasada „dwóch osób" - przykład rozdzielenia obowiązków. Zasada ta jest szczególnie ważna, gdy każdy może modyfikować infrastrukturę bezpieczeństwa, alarmy lub dzienniki zdarzeń. Zasada dwóch osób mówi, że każda modyfikacja systemu bezpieczeństwa wymaga współpracy dwóch upoważnionych osób i zawsze będzie istniała ścieżka audytu pokazująca, kto co zrobił i kiedy. Ta procedura jest również używana, gdy dwie lub więcej grup jest współodpowiedzialnych za wspólne elementy systemu bezpieczeństwa.

Poufne szczegóły projektu

Często innym jest łatwo zlokalizować i zidentyfikować krytyczne komponenty infrastruktury. Często informacje są wyraźnie pokazane w dokumentach publicznych. Oznakowanie na lokalizacjach infrastruktury często jasno opisuje, co jest w środku, a krytyczne komponenty są często umieszczane

w miejscach łatwo dostępnych dla osób postronnych. To wszystko są niebezpieczne praktyki projektowe. Wiele typów dokumentów wyraźnie wskazuje obszary SI, systemy wsparcia i inną infrastrukturę. Dokumenty mogą wskazywać lokalizację sprzętu, okablowania, mediów i tras kablowych. Dokumenty, które mogą ujawnić poufne informacje, obejmują plany budynków przedstawiające układy pięter i biur, meble, okablowanie i lokalizację wyposażenia. Dokumenty architektoniczne i inżynieryjne, rysunki i specyfikacje często zawierają poufne informacje. Dokumenty te często wymieniają funkcje każdego obszaru, a nawet nazwisko lub stanowisko kupującego. Inne rodzaje dokumentów również naruszają bezpieczeństwo. Przykładami mogą być plany powykonawcze, plany zmian i budowy, schematy okablowania elektrycznego i komunikacyjnego, konfiguracje paneli krosowniczych i połączeń krzyżowych, a także rysunki kontraktowe lub propozycje, rysunki warsztatowe, plany instalacji, schematy konserwacji, a zwłaszcza dokumenty. złożone w agencjach zajmujących się przestrzeganiem kodeksu i organami regulacyjnymi. Dobra ochrona wymaga, aby wszystkie takie dokumenty były kontrolowane i bezpiecznie przechowywane. Co więcej, wrażliwe informacje powinny zostać usunięte, a oznaczenia alfanumeryczne, które są odsyłaczami do arkuszy, które można łatwo zachować jako tajne, powinny wymazać. Wszystkie wymienione dokumenty są rutynowo rozprowadzane do wielu różnych źródeł, takich jak zainteresowani wykonawcy i oferenci, sprzedawcy, dostawcy i dostawcy usług konserwacyjnych. Menedżerowie budynków, właściciele i często biura nieruchomości prawdopodobnie przechowują kopie plików, a wiele innych osób może łatwo uzyskać dostęp do dokumentów i je kopiować. Większość takich dokumentów jest publicznie dostępna lub możliwa do uzyskania dzięki prawu słońca, orzeczeniu sądu lub po prostu podstępem. Ponadto wiele uprawnionych osób uzyskujących lub otrzymujących dokumenty nie ma wewnętrznej kontroli dokumentów ani przepisów dotyczących bezpieczeństwa. Wszystkie oznaczenia pomieszczeń i obszarów powinny być zawsze alfanumeryczne. W żadnym obszarze nie należy używać nazw opisowych ani funkcjonalnych. To zastrzeżenie dotyczy całego lokalu, wszystkich obszarów publicznych obiektu oraz wszystkich części mechanicznych i kluczowych budynku. Funkcjonalne określenia lub terminy, takie jak „skarbnik", „dyrektor ds. Marketingu", „biurko ochrony", „sala komputerowa", „szafa sieciowa" czy „pokój telefoniczny" nigdy nie powinny się pojawiać. Nie należy też podawać nazwisk żadnych mieszkańców, działów, grup funkcyjnych ani poszczególnych powierzchni najemców. Używaj tylko oznaczeń alfanumerycznych. Listy, które korelują numery powierzchni i pomieszczeń, obszary funkcjonalne lub wszelkie nazwy opisowe, powinny być przechowywane w bezpiecznym pliku, podobnie jak rysunki pomieszczeń wyposażenia, połączenia paneli krosowniczych i plany okablowania. Wszystko to musi być łatwo dostępne dla administratorów systemu w przypadku awarii systemu lub podczas wykonywania konserwacji lub uaktualnień, ale tylko wtedy, gdy jest to niezbędne. W idealnym przypadku nawet menedżerowie nie mają dostępu do tych informacji, chyba że towarzyszą im pracownicy ochrony. Oprócz kontroli dostępu do takich dokumentów równie ważne jest, aby każdy dokument był aktualny. Wreszcie, personel ochrony powinien przejrzeć wszystkie plany, rysunki i dokumenty dotyczące konstrukcji, zmian, przemieszczeń sprzętu lub wszelkich innych zmian fizycznych przed wydaniem informacji. Pracownicy ochrony powinni również przejrzeć zaproszenia do składania ofert oraz wszystkie rysunki i specyfikacje, ponownie przejrzeć otrzymane oferty i kontynuować przegląd każdego dokumentu powykonawczego wytworzonego w trakcie trwania projektu. Bezpieczeństwo wewnętrzne powinno dokonać przeglądu wszystkich tych kwestii w ramach polityki. Jeśli personel ochrony nie ma wystarczającej ilości czasu lub wiedzy, aby wszystko szybko i dokładnie przejrzeć, cenni mogą być niezależni eksperci z zewnątrz. Właściwie dobrani eksperci mogą zapewnić szerokie doświadczenie, perspektywę i dowody należytej staranności, tak aby kierownictwo nie mogło później zostać oskarżone o zaniedbanie w ochronie informacji, osób lub mienia. Wreszcie, lider ds. Bezpieczeństwa powinien potwierdzić, że żaden dokument projektu nie narusza żadnych wewnętrznych zasad bezpieczeństwa.

Trudności w ochronie infrastruktury.

Dziesiątki lat temu większość sprzętu IS znajdowała się w pojedynczej sali komputerowej, a większość zewnętrznych terminali i urządzeń peryferyjnych znajdowała się w pobliżu. Trasy kablowe były krótkie i generalnie w bezpiecznych obszarach, a kontrola dostępu, alarmy i nadzór mogłyby z łatwością objąć obszary krytyczne. Często byli też ochroniarze. Ale w tamtych czasach było mniej zagrożeń i mniej kosztów, jeśli pojawiały się problemy. Wiele organizacji było wtedy apatycznych, a bezpieczeństwo było luźne. Mieli szczęście, ale zdarzyło się kilka incydentów i często wiązało się to z dużymi kosztami. Prawdopodobnie było również wiele nieodkrytych naruszeń bezpieczeństwa, a jeszcze więcej, które nigdy nie zostały zgłoszone. Obecnie infrastruktura IS jest znacznie większa i bardziej złożona, a potencjalne koszty problemów są znacznie większe. Dzisiejsza infrastruktura jest znacznie bardziej współzależna i obejmuje teraz o wiele więcej urządzeń i pomieszczeń sieciowych. Rozciąga się na wiele innych szaf telefonicznych i użytkowych oraz łączy rozległe i zróżnicowane węzły stacjonarne, peryferyjne i zdalne. Dzisiejsza infrastruktura jest coraz trudniejsza do ochrony, a perspektywy na przyszłość sugerują o wiele więcej zagrożeń, które mogą spowodować poważne zakłócenia w działalności. Aby jeszcze bardziej skomplikować bezpieczeństwo, istnieje obecnie znacznie więcej różnorodnych interfejsów IS oraz złożona infrastruktura do ochrony. Interfejsy obejmują teraz okablowanie bezpośrednie i komutowane, topologie bezprzewodowe i sprzężenie w podczerwieni. Dostęp do Internetu, sieci lokalnych i rozległych może obecnie wykorzystywać kombinacje okablowania metalowego i światłowodów, połączeń bezprzewodowych, satelitarnych, telewizji kablowej i mikrofalowych. Niektóre z tych interfejsów będą dedykowane, inne przełączane, a jeszcze inne tymczasowo załatane. Trudno będzie nawet zlokalizować wszystkie interfejsy, ale każdy z nich musi być chroniony, podobnie jak ich kable i narzędzia, które je obsługują. Obecnie wczesne ostrzeżenia z alarmów bezpieczeństwa i obrony muszą być tak skuteczne, aby większości problemów można było zapobiec, zanim się pojawią.

Wygląd dobrego zabezpieczenia.

Pojawienie się uzbrojonej fortecy zwykle przynosi efekt przeciwny do zamierzonego. Zwykle bardziej onieśmiela i utrudnia zarówno gościom, jak i personelowi, niż ich chroni. To samo często dotyczy zbyt wielu strażników i recepcjonistów stacjonujących w celu blokowania wejść do obszarów wewnętrznych (chyba że zostanie to uznane za absolutnie konieczne). Takie bariery zwykle rozwścieczają każdego, kto już jest niespokojny i mogą sprowokować ataki. Bariery bywają nieskuteczne; na przykład, nawet jeśli szkło jest kuloodporne i bryzgoszczelne, otwory przelotowe prawdopodobnie nie są. Większość barier można również przełamać, a osoba (y) znajdująca się wewnątrz może doznać obrażeń lub przynajmniej doznać traumy. Na przykład kilka lat temu większość banków rzuciła się do umieszczania swoich kasjerów za grubymi szklanymi panelami. Wkrótce jednak odkryli, że szkło wywołuje kłopoty, a nie je odstrasza. Banki szybko usunęły zarówno szkło, jak i przepusty, które następnie kupiło i zainstalowało wiele firm, z podobnym skutkiem. Najlepszym sposobem uniknięcia gniewu i potencjalnej przemocy jest dobry projekt obiektów, systemy bezpieczeństwa i kontrola dostępu oraz szkolenia w zakresie świadomości bezpieczeństwa i zapobiegania przemocy. Istnieją również rozważania, czy urządzenia zabezpieczające powinny być ukryte lub widoczne na widoku dla wszystkich. Obrona, która jest widoczna, może służyć jako środek odstraszający i sprzyjać poczuciu bezpieczeństwa, ale może również sama być bezbronna. Aparaty mogą być malowane sprayem, wystrzeliwane lub strącane pałką. Wszelkie odsłonięte okablowanie (które samo w sobie jest zabezpieczeniem nie-nie) można przeciąć lub przebić. Alternatywą jest użycie ukrytych urządzeń, a także fałszywych urządzeń lub „honeypotów", które są oczywiście umieszczone.

Właściwe oznakowanie

Dobre bezpieczeństwo wymaga szybkiego zlokalizowania problematycznych miejsc, mając pewność, że nazewnictwo każdego komponentu, kabla i złącza jest przejrzyste i aktualne. Musi istnieć odpowiednie i spójne oznakowanie wszystkich kabli danych i zasilających, zarówno wewnątrz, jak i poza strefami bezpiecznymi. Żadna etykieta ani oznaczenie nie powinny ujawniać informacji poufnych. Wielu dostawców, instalatorów, pracowników kontraktowych i pracowników wewnętrznych ma tendencję do stosowania własnych systemów etykietowania i etykietowania, z których niektóre są jasne i zrozumiałe, a inne nie. Etykietowanie i oznaczanie muszą być zgodne z dokumentacją, planami i rysunkami. Niedbałe zarządzanie okablowaniem jest często normą, ponieważ zmiany są wprowadzane, ale nie są oznaczane ani dokumentowane, lub porzucane i nie usuwane okablowanie. Status personelu wewnętrznego, instalatorów i konserwatorów prawdopodobnie będzie się często zmieniać, stwarzając tym większe potencjalne źródło dezinformacji i zamieszania. Nieuniknionym skutkiem jest słaba ochrona i powolna reakcja na incydent bezpieczeństwa. Istnieją ogólnie przyjęte procedury zarządzania przewodami i jedna metoda powinna być stosowana w całej infrastrukturze informacyjnej. Szczególnie ważne jest, aby wszyscy upoważnieni pracownicy rozumieli i akceptowali system etykietowania.

Stowarzyszenie Przemysłu Telekomunikacyjnego / Electronic Industry Alliance (TIA / EIA) publikuje ogólnie przyjęty organ, TIA / EIA Standard 606-B, Administration Standard for the Telecommunications Infrastructure , który opisuje oznaczanie kabli, złączy, paneli krosowych, połączeń krzyżowych, i wyposażenie. Norma ta wymaga również etykietowania ogniochronnych, uziemień, specjalnych obwodów uziemienia i przewodów neutralnych. National Electric Code (NFPA 70), 10 opublikowany przez National Fire Protection Association, zawiera również normy dotyczące oznaczania kabli i przewodów. Kody lokalne mogą uzupełniać kody krajowe. Ogólnie rzecz biorąc, wszelkie istotne przeróbki, przeprowadzki lub zmiany, i zazwyczaj każda nowa konstrukcja będą wymagały pełnej zgodności z obowiązującymi normami w całym obiekcie - co jest również rozsądną inwestycją w bezpieczeństwo.

Niezawodność i nadmiarowość

Pierwszym warunkiem niezawodnego działania systemu jest niezawodny sprzęt, systemy i infrastruktura, prawidłowo zainstalowane i utrzymywane. Niestety, niektóre elementy mogą być źle zaprojektowane, poddawane błędnej kontroli jakości, uszkodzone podczas transportu lub nieprawidłowo zastosowane. Wiele urządzeń zawiera teraz tryb awaryjny, aby zachować pełną wydajność w przypadku awarii. Kolejnym składnikiem wysokiego poziomu usług jest nadmiarowość: współbieżnie dostępny sprzęt i równoległe ścieżki przejmowania obciążenia w przypadku awarii jednego z elementów. Skuteczna nadmiarowość zapewniająca ciągłość biznesową wymaga również innych lokacji, które są poza lokalem, aby przetwarzać i przechowywać informacje. Najlepiej, aby istniało wiele alternatywnych lokacji, każda w bezpiecznym środowisku i dobrze odległa, tak aby problemy w lokacji głównej nie wpływały na żadne inne. W każdym pomieszczeniu komputerowym systemy pamięci masowej powinny być nadmiarowymi macierzami niezależnych dysków (RAID), umożliwiającymi pełną replikację ważnych danych. W przypadku danych krytycznych same systemy pamięci masowej RAID powinny być nadmiarowe. Serwery również powinny być nadmiarowe. Wiele serwerów równoległych z równoważeniem obciążenia to rozsądna inwestycja, tak aby jeden serwer automatycznie przejmował obciążenie innego, jeśli z jakiegoś powodu się zawiesza lub musi przejść w tryb offline. Funkcje równoważenia obciążenia zapewniają również potencjalnie wyższą przepustowość dla całego systemu, umożliwiając równoległe obliczenia i operacje wejścia / wyjścia. Wszystkie krytyczne urządzenia powinny mieć nadmiarowe zasilacze, wentylatory i dyski twarde, które można szybko zdiagnozować i łatwo wymienić. Dobre zarządzanie systemem to kolejny ważny wymóg. Obejmuje to sprzęt, który może wykryć problem przed jego wystąpieniem i, jeśli to możliwe, wskazać

dokładną lokalizację. Zawiera również dobre oprogramowanie do zarządzania z funkcjami ostrzegania i alarmowania oraz dobre systemy logowania. Możliwości zdalnego zarządzania również muszą być prywatne i bezpieczne, aby wykluczyć ataki penetracyjne lub ataki typu „odmowa usługi". Dobre zarządzanie bezpieczeństwem wymaga również, aby każda zmiana lub wyłączenie parametrów alarmowych wymagała fizycznej obecności dwóch upoważnionych osób w pomieszczeniu sprzętowym i jednoczesnego zalogowania się. Dobre zarządzanie systemem wiąże się z pewnym kosztem, ale jest rozsądną inwestycją w skuteczne zabezpieczenia i nadzór

Prawidłowa instalacja i konserwacja

Dobra ochrona wymaga prawidłowego zainstalowania wszystkich systemów informacyjnych, sprzętu i okablowania, zgodnie z instrukcjami producenta i przeznaczeniem. Całe okablowanie musi spełniać lub przekraczać wymagania przepisów lokalnych. Okablowanie danych powinno być niezależnie testowane i certyfikowane, że spełnia specyfikacje, aktualne standardy i, jeśli to możliwe, przewidywane przyszłe potrzeby. Niestandardowe podłączenia i instalacje sprzętu są powszechne i są przyczyną wielu awarii systemu. Większość funkcji bezpieczeństwa jest wyłączana, gdy dostarczane są komponenty i oprogramowanie. Prawidłowa instalacja wymaga starannej konfiguracji, dostosowania i testów wydajności, na które należy przeznaczyć odpowiednią ilość czasu i zasobów. Szybkie instalowanie najnowszych modyfikacji, dodatków Service Pack, aktualizacji i poprawek zabezpieczeń ma również kluczowe znaczenie dla utrzymania wydajności. Często interweniują opóźnienia trwające dni, tygodnie, a nawet miesiące, podczas gdy pojawiają się nowe zagrożenia lub ich poziomy eskalują, aż do wprowadzenia nowych zabezpieczeń. Po zainstalowaniu systemy informacyjne i infrastruktura muszą być okresowo przeglądane, testowane i aktualizowane. Częstotliwość takich przeglądów i testów musi odzwierciedlać znane lub szacowane wskaźniki awarii i konsekwencje takich awarii. Administratorzy, personel zajmujący się instalacją i konserwacją muszą być odpowiednio przeszkoleni, doświadczeni, a w wielu przypadkach także certyfikowani lub licencjonowani. Poświadczenia każdej osoby należy sprawdzić, zanim zostanie wpuszczona na teren zakładu. Biorąc pod uwagę ograniczoną liczbę pracowników, czas i dostępne budżety, w procesie zapewniania niezawodności często występuje więcej deklaracji niż faktycznej pewności. Kierownictwo musi zrozumieć, że właściwa instalacja, utrzymanie i konserwacja razem stanowią tanią i skuteczną gwarancję, że wydajność IS nigdy nie zostanie zagrożona.

INNE UWAGI

Istnieje wiele innych czynników, które mogą znacząco wpłynąć na ustanowienie i poprawę bezpieczeństwa fizycznego. Kilka z nich omówiono w następnych sekcjach.

Szafy na sprzęt

Większość urządzeń IS jest teraz montowana w stojaku otwartym, aby zaoszczędzić miejsce na podłodze, zapewnić bardziej niezawodne działanie i łatwiejszy dostęp. Chociaż zamknięte szafy sprzętowe kosztują więcej niż regały, zapewniają znacznie lepszą ochronę. Sprzęt zamontowany w zamkniętej szafce może być lepiej wentylowany i chłodzony, chroniony przed zanieczyszczeniami, a także może uniknąć uszkodzeń spowodowanych przez zewnętrzne cząstki, wodę, dym lub płyny. Jeśli kiedykolwiek dojdzie do przegrzania lub wytworzenia dymu w zamkniętej szafce, stan ten można szybko wykryć i zwykle rozwiązać, zanim sprzęt lub okablowanie ulegną uszkodzeniu. Zamki uniemożliwiają osobom nieuprawnionym lub przynajmniej opóźniają dostęp i pozostawiają ślady kłopotów. Alarmy przy otwartych drzwiach zapewniają kolejną silną warstwę ochrony, a kanały kablowe do szaf mogą być również chronione. Szafy z nadmiarowymi wentylatorami mogą lepiej monitorować i utrzymywać wentylację i chłodzenie, co z kolei ułatwia montaż większej liczby urządzeń

na mniejszej powierzchni. W sumie zamknięte szafy mogą zapewnić dodatkową warstwę ochrony przed przypadkowym lub umyślnym uszkodzeniem infrastruktury.

Dobre praktyki porządkowe

Wszelką żywność i napoje należy trzymać z dala od pomieszczeń ze sprzętem, ponieważ rozlanie ich na sprzęt, monitor, klawiaturę, złącza oraz okablowanie i wiązki przewodów może spowodować znaczne uszkodzenia. Jedzenie przyciąga także owady i gryzonie (które występują w wielu budynkach), z których wiele lubi również zjadać przewody. Ponadto, tłuszcz i inne zanieczyszczenia z żywności mogą być łatwo rozprowadzane przez operatorów na krytycznych powierzchniach sprzętu, takich jak urządzenia wejściowe i wyjściowe, i powodować błędy odczytu / zapisu, a nawet całkowite wyłączenie urządzeń. Na przykład, jedna zatłuszczona płyta DVD może zepsuć jednostkę DVD lub jednostkę taśmy kopii zapasowej o dużej pojemności. Co gorsza, zanieczyszczona głowica odczytu / zapisu lub szczelina wejściowa może z kolei przenosić zanieczyszczenie na inne nośniki, a następnie na inne urządzenia. Miejsce na jedzenie i napoje powinno być zapewnione poza pomieszczeniem wyposażenia, gdzie personel rutynowej konserwacji może utrzymywać obszar żywności w czystości. Wygodny dozownik do chusteczek do rąk na bazie alkoholu może zachęcić do czystości każdego wchodzącego do pomieszczenia z wyposażeniem. Luźne papiery, książki, materiały eksploatacyjne, gazety i śmieci stanowią zagrożenie pożarowe, a także muszą być wyrzucone z każdego pomieszczenia z wyposażeniem.

Ochrona jawna, ukryta i oszukańcza.

Skuteczna ochrona infrastruktury IS wymaga wielu ukrytych elementów - takich jak ukryte kamery monitorujące, czujniki i detektory - oraz całego okablowania, które je obsługuje. Ale dobra ochrona wymaga również kilku dobrze widocznych elementów. Ważne jest, aby zastanowić się, które urządzenia są najlepiej ukryte, aby je chronić, a które powinny być widoczne jako środki odstraszające. Urządzenia jawne to takie, które są widoczne dla pracowników i gości lub których obecność jest sugerowana przez inne widoczne przedmioty, takie jak tablice ostrzegawcze. Te widoczne urządzenia, które sugerują, że istnieje jakieś zabezpieczenie, mają na celu odstraszenie wichrzycieli, tak aby wszyscy oprócz najbardziej zdeterminowanych napastników udali się gdzie indziej. Przykładami są kamery monitorujące, kontrola dostępu, widoczne skrzynki alarmowe i widoczne czujniki. Chociaż większość jawnych urządzeń jest aktywnych i rejestruje dane, niektóre mogą być niedrogimi urządzeniami zastępczymi, które tylko wyglądają realnie, być może z wolno migającymi lampkami kontrolnymi, aby wzmocnić efekt. Ukryta ochrona nie może być jednak widoczna ani dla gości, ani osób wtajemniczonych. Nic nie może wskazywać, że te zabezpieczenia istnieją, czym są, jak mogą funkcjonować lub gdzie się znajdują. Najbardziej efektywne systemy bezpieczeństwa działają w ukryciu; przykłady obejmują ukryte i ciche alarmy, ukryte systemy wczesnego ostrzegania, czujniki obwodowe i zbliżeniowe, monitory dostępu i wiele innych urządzeń monitorujących, których nie widać. Ważne jest również, aby ukryć okablowanie, które łączy wszystkie systemy ochronne i obsługujące je media. Niezależnie od tego, czy jakakolwiek część systemu jest widoczna, czy nie, okablowanie, które ją łączy, nie powinno być. Chociaż jawne urządzenia mogą same w sobie być podatne na ataki, generalnie będą reklamować, że jest tu dobra ochrona i każdy w obiekcie może czuć się bezpiecznie. Jednak widoczne urządzenia mogą być czasami zakryte lub pomalowane w sprayu, strącone pałką lub wystrzelone, aby je wyłączyć. Doświadczony złodziej może również pokonać wiele ukrytych systemów, jeśli wie, czym one są, gdzie się znajdują lub w jaki sposób są połączone. Inne podejście do ochrony obejmuje oszustwa. Fikcyjne urządzenia, które wyglądają jak kamery monitorujące, urządzenia kontroli dostępu i czujniki alarmowe, można umieścić w taki sposób, aby przyciągnąć wichrzycieli, którzy mogą pomyśleć, że mogą fizycznie uszkodzić, wyłączyć lub obejść system. Te widoczne urządzenia mają na celu odwrócenie uwagi potencjalnych wichrzycieli i odwrócenie ich od wrażliwych obszarów. Niektóre

urządzenia są zwodnicze, ponieważ nie są tym, czym się wydają, ale w rzeczywistości są czujnikami alarmowymi do pomiaru ruchu, bliskości, dźwięku lub wszystkiego, co zakłóca działanie urządzenia. Podstępne urządzenia są często używane w celu odwrócenia wichrzycieli z dala od osób narażonych na niebezpieczeństwo i infrastruktury, oferując im „honeypot": atrakcyjny cel, który odwraca ich uwagę, ale często cel wyposażony w urządzenie alarmowe, kamery monitorujące lub inne sposoby identyfikacji sprawcy i zbieranie dowodów. Istnieje szara strefa między tym, co kierownictwo może zgodnie z prawem zrobić, aby chronić swoje systemy informacyjne, a tym, co może być nieetyczne lub niezgodne z prawem. Kierownictwo ma prawny i powierniczy obowiązek ochrony ludzi i mienia, a zwolennicy oszustwa twierdzą, że te techniki są coraz bardziej niezbędne do ochrony organizacji. Inni twierdzą, że jest to pułapka lub narusza prawa do prywatności. Stanowe i lokalne przepisy i interpretacje są bardzo zróżnicowane i podlegają ciągłym zmianom. Konieczne jest dokładne sprawdzenie z lokalnymi urzędnikami, doradcami prawnymi i ubezpieczycielami, aby określić, co jest dopuszczalne i jak zarządzać takim ryzykiem. Kierownictwo musi następnie zdecydować, w jakim stopniu te techniki mogą być skuteczne i czy wystarczą mniej kontrowersyjne podejścia. Niezależnie od tego, czy same urządzenia zabezpieczające są jawne, ukryte czy oszukańcze, systemy bezpieczeństwa za nimi nie mogą być oczywiste. Nikt, kto widzi lub wie o elementach systemu bezpieczeństwa, nie powinien być w stanie wydedukować szczegółów systemu, jego funkcjonalności ani miejsca i sposobu monitorowania. Obserwator może zauważyć określone urządzenie lub produkt lub sugestię standardowego rozwiązania zabezpieczającego dostawcy, ale szczegóły systemów ochrony muszą pozostać niejasne, a całe okablowanie, które je obsługuje, musi być ukryte lub zamaskowane. Wszyscy zaangażowani muszą znać zasady i procedury bezpieczeństwa. Widoczne znaki powinny informować, że każdy wchodzący na teren obiektu może być monitorowany, podobnie jak cała komunikacja. Wszystkie zasady i procedury bezpieczeństwa powinny być zrozumiane i zaakceptowane przez wszystkich zaangażowanych. Pracownicy i inny personel zakładowy powinni przechodzić okresowe szkolenia i instrukcje dotyczące bezpieczeństwa. Powinny istnieć okresowe ćwiczenia i ćwiczenia w zakresie bezpieczeństwa w celu przetestowania procedur i wzmocnienia szkolenia. Wreszcie ochrona nie może być nachalna. Bezpieczeństwo nie może w żaden sposób ograniczać produktywności ani wydajności IS. Zamiast tego ochrona musi przyczyniać się do poczucia bezpieczeństwa i ochrony w miejscu pracy, a tym samym zwiększać produktywność

KONTROLA DOSTĘPU

Systemy kontroli dostępu to tylko jedna warstwa dobrej ochrony infrastruktury. Są one zwykle używane w połączeniu z systemami nadzoru i kontroli obwodowej w celu zapewnienia dostatecznego wczesnego ostrzeżenia, aby zażegnać problemy, zanim się pojawią. Skuteczna kontrola dostępu wymaga trzech poziomów wsparcia, które zostały opisane poniżej. Siła każdego poziomu i jego integracja z innymi warstwami zabezpieczeń decyduje o skuteczności zabezpieczeń.

1. Przywileje. Poziom ten określa, czy osoba ubiegająca się o wpis jest upoważniona. Jest to proces wstępnego żądania wejścia, który może wykorzystywać kartę dostępu lub kartę zbliżeniową, klucz identyfikacji radiowej (RFID) lub zamek szyfrowy. Ponieważ wiele z tych urządzeń można zgubić, pożyczyć, skraś lub skopiować, a wiele z nich można szybko pokonać, zwykle nie ma wiele wysiłku, aby ustalić, kto właśnie szuka dostępu. Dlatego same przywileje nie są silnym zabezpieczeniem.

2. Uwierzytelnienie. Zazwyczaj konieczna jest pewna identyfikacja osoby starającej się o wjazd. Aby to zrobić, osoba musi posiadać lub wiedzieć coś wyjątkowego, czego inni nie mogą łatwo skopiować. Przykłady obejmują osobiste numery identyfikacyjne (PIN), klucze elektroniczne, karty wstępu i urządzenia biometryczne. Można używać kodów PIN i haseł, pod warunkiem, że są mocne i dobrze wdrożone. Niektóre z tych podejść jedynie wzmacniają proces przywilejów, ale nadal można je skopiować lub pokonać.

3. Ścieżka audytu. W przypadku każdej próby wpisu wymagany jest dziennik, który zawiera datę i godzinę, dane identyfikacyjne osoby oraz działania podjęte przez system kontroli dostępu. Zdarzenia odmowy dostępu i niemożności zidentyfikowania powinny wywołać natychmiastowe alarmy. Dzienniki muszą być analizowane w odpowiednim czasie pod kątem anomalii lub nietypowych wzorców. Tam, gdzie potrzebna jest lepsza kontrola dostępu, wyjście każdej osoby również musi zostać uwierzytelnione i zarejestrowane.

Zamki i sprzęt

Silna ochrona zaczyna się od wysokiej jakości zamków, okuć do drzwi i systemów kontroli dostępu, które są nieinwazyjne, ale wystarczająco mocne, aby powstrzymać większość osób nieupoważnionych. Typy zamków powinny być trudne do wybrania i powinny używać kluczy, które są trudne do skopiowania. Przykładami są zamki i klucze Medeco z wgłębieniami po bokach. Zamki Ace R z okrągłymi wpustami wymagają specjalnych narzędzi do otwierania. Z numerów zamków można utworzyć wiele typów kluczy, dlatego należy je bezpiecznie przechowywać. Żaden zamek nie jest całkowicie bezpieczny. Ktoś dysponujący sprzętem, doświadczeniem i czasem może otworzyć każdy zamek, często bardzo szybko i bez zwracania uwagi. Tam, gdzie stosowana jest kontrola klucza, doświadczona osoba z kluczem do jednych drzwi może otworzyć wkładkę bębenkową i skopiować system kontroli. Dlatego potrzebne są dodatkowe warstwy ochrony. Obszary wewnętrzne, do których dostęp ma tylko kilka osób, zwykle można zabezpieczyć mocnym zamkiem szyfrowym z przyciskiem. Zamki na klucz nie są odpowiednie, ponieważ klucza nie można zmieniać okresowo ani szybko, gdy klucz zostanie zgubiony lub ktoś wyjdzie. Zagubione lub zgubione klucze mogą nie zostać zgłoszone przez kilka dni lub tygodni. Jednak zamki na klucze są zwykle mocniejsze i mniej podatne na wandalizm, więc klucze mogą być najlepszą alternatywą do obszarów zewnętrznych lub do drzwi, które pozostają otwarte w godzinach pracy. Wszędzie tam, gdzie klucz uzyskuje dostęp do krytycznych obszarów, na miejscu powinny znajdować się zapasowe wkładki bębenkowe i nowy zestaw kluczy, które można szybko wykorzystać, gdy zajdzie potrzeba wymiany. Po wymianie wkładki bębenkowej stary wkład należy przeładować i wyprodukować nowy komplet kluczy. Szczególnie skuteczne są zamki z kluczem elektronicznym. Siłowniki aktywowane elektronicznie mogą zastąpić istniejące cylindry mechaniczne, a wiele z nich nie wymaga żadnego okablowania, więc sprzęt i koszty operacyjne są minimalne. Większość kluczy elektronicznych ma małą cylindryczną końcówkę, którą dotyka się zamka w celu uzyskania dostępu. Zarówno zamek, jak i klucz mogą rejestrować każde zdarzenie, identyfikować konkretny używany zamek lub klucz, datę i godzinę oraz to, czy udzielono dostępu. I wygodnie, klucze elektroniczne nie są dużo większe niż klucze mechaniczne. Jednak oba można pokonać przy użyciu odpowiedniego sprzętu i umiejętności. Często stosuje się dwa niezależne zamki wjazdowe, aby zapewnić silniejszą, stosunkowo niedrogą ochronę. Urządzenia RFID mogą zapewnić dobrą kontrolę dostępu, pod warunkiem, że urządzenie aktywujące nie zostanie zgubione lub skradzione. RFID może być ulepszeniem w stosunku do systemów wprowadzania kart, ponieważ może aktywować zamek z odległości kilku stóp. Karty dostępu RFID mogą zawierać identyfikator ze zdjęciem, nazwisko i być może pasek optyczny do zaszyfrowanych informacji o tożsamości. Podobnie jak w przypadku innych systemów, RFID można złamać przy użyciu odpowiedniego sprzętu i umiejętności. Innym niedrogim ulepszeniem zamków na klucz jest blokada dostępu do karty, podobna do tych stosowanych w hotelach. Wiele z nich nie wymaga okablowania i działa na baterie, więc klucz do każdych drzwi pozostaje niezmieniony, a stary klucz pozostaje ważny. Dlatego bez centralnego okablowania większość zamków z dostępem do karty zapewnia ograniczone bezpieczeństwo i nie może wywołać alarmu, chociaż niektóre przynajmniej rejestrują zdarzenia. Aby uniemożliwić intruzom ominięcie mechanizmów zamka przez użycie kart kredytowych lub cienkich blach do wepchnięcia rygli do wewnątrz, obszar nad rzeczywistym zatrzaskiem powinien być zabezpieczony szczebliną - metalową klapą przykręconą do drzwi. Ponadto zatrzaski powinny mieć zabezpieczenia przed manipulacją, które blokują zewnętrzny ruch elementów

ruchomych do drzwi, gdy zamki są aktywne. Zawiasy do drzwi nie powinny być dostępne z zewnątrz zabezpieczonego obszaru, gdy drzwi są zamknięte: Łatwo jest złamać i wyjąć śruby zawiasów i zdjąć zamknięte drzwi, jeśli zawiasy są na zewnątrz. Niezależnie od tego, jak silne są systemy kontroli dostępu, drzwi mają swoje ograniczenia. Bez drzwi i okuć typu krypty, zdeterminowany napastnik z pistoletem i tłumikiem może łatwo uzyskać dostęp. Mała armatka wodna, która jest przewożona w czymś, co wygląda jak skrzynka z narzędziami, może jednym strzałem i bardzo małym hałasem złamać standardowe metalowe drzwi lub otaczającą je przegrodę.

Systemy wprowadzania kart

Jednym z najlepszych środków fizycznej kontroli dostępu jest system wprowadzania kart, zwłaszcza nowsze systemy, które są coraz bardziej wydajne i mniej kosztowne. Centralny system wprowadzania kart często kontroluje cały obiekt: wszystkie wejścia, wyjścia, windy, toalety i wiele innych drzwi wewnętrznych. Karty dostępu są zwykle podobne do kart kredytowych i można je nosić schowane lub noszone jako identyfikatory. Karty dostępu są zwykle nadrukowane ze zdjęciem całej twarzy, nazwiskiem osoby, logo organizacji, a często z wydrukowanym paskiem z danymi biometrycznymi. Karty dostępu często zawierają kody numeryczne wskazujące autoryzowane obszary dostępu i są zwykle oznaczone kolorami w celu wskazania statusu i tego, czy dana osoba musi być eskortowana.

Karty zbliżeniowe i dotykowe

Niektóre karty można trzymać w pobliżu czujnika (karty zbliżeniowe), a inne w kontakcie z czujnikiem (karty dotykowe). Oba typy żetonów mogą zmniejszyć zużycie fizycznych żetonów, które należy umieścić bezpośrednio w kontakcie z czujnikami

Uwierzytelnianie

Każdy może skorzystać z tokena kontroli dostępu, który może zostać wypożyczony, zgubiony, skopiowany, zmieniony, skradziony lub zabrany siłą. Dlatego uwierzytelnianie jest kolejną warstwą bezpieczeństwa potrzebną do ustalenia tożsamości osoby ubiegającej się o wpis z pewnym stopniem pewności. Urządzenia uwierzytelniające zwykle obejmują skaner biometryczny, klawiaturę numeryczną oraz identyfikację wizualną lub głosową przez komputer lub inną osobę. Wszystkie takie urządzenia mają różne poziomy zabezpieczeń i każdego z nich można używać łącznie. Podczas odczytywania tokenu dostępu system musi sprawdzić, czy token ma wymagane uprawnienia dla tego miejsca, daty i godziny. Jeśli tak, wówczas konieczne staje się uwierzytelnienie tożsamości osoby korzystającej z tokena. W tym celu klawiatura numeryczna była niegdyś najpopularniejszym urządzeniem, za pomocą którego użytkownik tokena wprowadzał swój identyfikator na klawiaturze numerycznej. Obecnie większość korzysta z ekranu dotykowego, na którym liczby pojawiają się w losowej kolejności. Jeśli system zatwierdził kod PIN, aktywował elektryczny zamek do drzwi, aby chwilowo odblokować drzwi. Ten system może być powolny, nieporęczny i łatwy do złamania. W niektórych systemach wszyscy używają tego samego kodu PIN i powinni zachować prywatność. Jednak kody PIN mogą zostać zapomniane, zgubione lub odkryte przez innych. Uwierzytelnianie wizualne to lepsze podejście. Może to zrobić komputer lub ochroniarz lub recepcjonista, który może obserwować wejście lub monitorować je za pomocą kamery monitorującej lub wideodomofonu. Wideodomofony typu awaryjnego działają dobrze, ponieważ zapewniają zdalne uwierzytelnianie za pomocą obrazu wizualnego i mogą monitorować dźwięk w sposób ciągły, dzięki czemu osoba uwierzytelniająca może rozmawiać i rzucać wyzwanie każdemu, kto zbliża się do drzwi. Po zweryfikowaniu tożsamości system lub inna osoba aktywuje się elektrozaczep do otwierania drzwi. Ten system zapewnia większe bezpieczeństwo i jest szybszy niż klawiatura. Ułatwia również rejestrowanie i rejestrowanie wszystkich wejść i wyjść, zwłaszcza poza godzinami pracy. Naruszenia mogą się zdarzyć, jeśli osoba ubiegająca się o wejście może oszukać strażnika lub recepcjonistkę. Skanery biometryczne zapewniają najsilniejsze

zabezpieczenia. Oferują szybszą, bardziej pozytywną identyfikację każdej osoby i eliminują konieczność zapamiętywania kodu PIN. Skanery biometryczne mogą odczytać każdy z tych osobistych atrybutów, które są wymienione nieco w kolejności ich aktualnej popularności: wzory odcisków palców, cechy twarzy, odcisk głosu, odcisk dłoni, podpis, szczegóły siatkówki lub wzrost i waga. Większość systemów biometrycznych można dostosować tak, aby były bardzo czułe (wolniejsze i mogą wymagać wielokrotnych prób wejścia, ale bardzo trudno je złamać) lub mniej czułe (co nadal jest szybkie, ale może skutkować fałszywymi uwierzytelnieniami). Przed wyborem systemu biometrycznego należy ustalić, czy użytkownicy go rozumieją i akceptują. Na przykład niektórzy ludzie wzbraniają się przed koniecznością korzystania ze skanera siatkówki, podczas gdy inni mogą uważać, że jakiekolwiek urządzenie biometryczne narusza ich prywatność. Drugi powód jest nieważny, ponieważ większości systemów biometrycznych nie można użyć do identyfikacji żadnej osoby, która nie jest jeszcze znana w systemie. Coraz częściej, zwłaszcza w krytycznych miejscach publicznych, systemy te mogą sprawdzać każdą osobę w bazach danych przestępców i terrorystów oraz szybko ostrzegać organy ścigania. Trudno jest ukraść tożsamość za pomocą biometrii, ponieważ trzeba również znać zastosowane algorytmy kodowania. Skanery linii papilarnych są najpopularniejsze i mają coraz większe możliwości. Początkowo wykorzystywały one skanowanie optyczne, które można było oszukać fotografiami, odciskami wosku lub odciętą cyfrą. Nowsze skanery pojemnościowe wykorzystują raczej elektronikę niż optykę i mogą zapewnić prawie pewną identyfikację. Zazwyczaj trzy palce użytkownika są „rejestrowane" w systemie na wypadek, gdyby niektóre palce zostały później zabandażowane lub zabrudzone. Jeśli wszystkie zarejestrowane palce są niezdolne do wyrażenia zgody, do obejścia systemu można użyć haseł jednorazowych. Większość skanerów linii papilarnych nie jest w stanie zidentyfikować osoby po nazwisku, a jedynie osoba ubiegająca się o wjazd odpowiada osobie, której tożsamość biometryczna została zarejestrowana. Większość skanerów nie jest zgodna z jednolitymi standardami automatycznej identyfikacji odcisków palców stosowanymi przez organy ścigania. Zamiast tego skanują niewielki obszar palca i stosują zastrzeżone algorytmy i szyfrowanie. Szablon z jednego systemu jest zwykle bez znaczenia dla innego. Na dokładność skanowania odcisków palców ma wpływ kąt i położenie palca oraz zastosowany nacisk. Większość systemów umożliwia dostosowanie czułości, aby zoptymalizować czasy rejestracji i weryfikacji oraz wskaźniki sukcesu, a także zminimalizować opóźnienia i fałszywie ujemne wyniki, które wymagają wielokrotnych prób dostępu. Chociaż dobrze sprawdzają się w większości zastosowań, skanery linii papilarnych mogą nie być odpowiednie w przypadku, gdy użytkownik może mieć brudne lub mocno zrogowaciałe ręce lub musi nosić rękawiczki (np. pracownicy służby zdrowia). Rozpoznawanie twarzy to podstawa innego popularnego systemu skanowania. Wykorzystuje technologie graficzne i dowolną kamerę monitorującą do pomiaru wielkości i relacji widocznych elementów twarzy. Większość systemów jest zastrzeżonych i nie można ich używać do identyfikacji osób po imieniu, ale niektóre inne są zgodne ze standardami organów ścigania. Czułość i dokładność zależą od odległości, położenia i kąta nachylenia głowy, a także od oświetlenia tła. Aparaty we wszystkich punktach wejścia muszą być ustawione tak, aby fotografować obiekt pod tym samym kątem, pod jakim zostały zarejestrowane ich twarze. Nie wszystkie systemy rozpoznawania twarzy zapewniają silne zabezpieczenia; niektórych można oszukać maską na twarz lub fotografią. Inne najlepiej pozostawić przy najwyższych ustawieniach czułości, aby uniknąć fałszowania, co może wymagać większej liczby fałszywych alarmów i wielu prób wejścia. Można użyć skanowania głosowego, ale głównie w celu uzyskania dostępu do terminala lub stacji roboczej. Lepsze systemy wyświetlają losowe słowa na monitorze, więc nie można użyć wstępnie zarejestrowanej odpowiedzi. Większość korzysta z mikrofonu stacji roboczej lub, coraz częściej, telefonu komórkowego. Chrypka może wpływać na skanery głosu, dlatego należy zapewnić jednorazowy dostęp do hasła. Systemy te mogą być przydatne do zdalnego logowania, zwłaszcza podczas podróży, chociaż niska przepustowość obwodów telefonicznych może zmniejszyć użyteczność systemu. Skanery siatkówki lub tęczówki są uważane za najlepsze zabezpieczenia, ale uwierzytelnianie

może zająć kilka sekund. Aby uzyskać kontrolę dostępu, użytkownik musi na ogół uważnie patrzeć w okular, co dla niektórych osób jest traumatyczne. Jednak aby uzyskać dostęp do terminala lub stacji roboczej, kamera internetowa jest zwykle umieszczana na monitorze, w odległości od 17 do 19 cali od oka. Głowa użytkownika musi być ustawiona tak, aby wyrównać białą kropkę w kolorowym okręgu. Użytkownik musi stać nieruchomo, bez mrugania, podczas gdy skanowanie przebiega automatycznie. Kamery można używać do nadzoru, aby zobaczyć, kto znajduje się w pobliżu stacji roboczej.

Zintegrowane systemy dostępu

Skanery biometryczne są coraz częściej używane przez inne aplikacje i większość z nich może łatwo współpracować z systemem kontroli dostępu. Aplikacje obejmują autoryzację użytkowników sieci, dostęp do terminali i stacji roboczych oraz do aplikacji i danych. Czytniki biometryczne można wbudować w laptopy, klawiatury, myszy lub czytniki peryferyjne. Mogą być używane z kartami dostępu, identyfikatorami i urządzeniami zbliżeniowymi lub RFID do uwierzytelniania z pewnym stopniem pewności. Skanery, które są w większości zastrzeżone, są obecnie zintegrowane z systemami szyfrowania (np. Wirtualnymi sieciami publicznymi, infrastrukturą klucza publicznego i kartami inteligentnymi) w celu uwierzytelniania transakcji, w tym kart kredytowych, finansowych, bankowych i bankomatów. Biometria jest coraz częściej wykorzystywana do identyfikacji pacjentów szpitalnych, odbiorców świadczeń socjalnych, osób, które często przyjeżdżają do Stanów Zjednoczonych, oraz podobnych zastosowań, które obejmują identyfikację zróżnicowanej lub szeroko rozproszonej grupy. Ochrona bezpieczeństwa infrastruktury może być niezależna lub zintegrowana z kompleksowym systemem bezpieczeństwa pomieszczeń. Karty lub identyfikatory mogą zapewnić wiele innych funkcji wykraczających poza podstawową kontrolę dostępu. Aplikacje obejmują dostęp do budynku, wind i lokali poza godzinami pracy; kontrola wejść do budynków, toalet i parkingów (zwłaszcza w nocy); zakupy w kafeterii lub sklepie firmowym lub w celu ładowania artykułów papierniczych lub materiałów odebranych z magazynu. Mogą być również wykorzystywane do otrzymywania dokumentów niejawnych. Aby zapewnić większą ochronę i wydajność, zintegrowany system sieciowy obejmujący całe przedsiębiorstwo może kontrolować dostęp do różnych pomieszczeń, zamkniętych drzwi, elementów infrastruktury, sieci, stacji roboczych, aplikacji, bezpiecznych danych i połączeń internetowych. Takie rozwiązanie zapewnia pełne bezpieczeństwo dzięki rejestrowaniu każdego zdarzenia. Scentralizowane dzienniki mogą dostarczyć znacznie bardziej znaczących informacji o bezpieczeństwie, ponieważ zintegrowany system zapewnia lepsze wczesne ostrzeżenia, aby zapobiec problemom, zanim się pojawią.

Maszyny portalowe

Punkty kontroli bezpieczeństwa podobne do lotnisk są coraz częściej instalowane poza lotniskami. Maszyna portalowa to brama, przez którą trzeba przejść podczas procedury bezpieczeństwa na lotnisku. Wykrywa ukryty metal, taki jak pistolety i noże oraz narzędzia, które mogą być używane do powodowania problemów. Portal może być używany do wykrywania elementów IS (takich jak nośniki danych) przemycanych do lub z lokalu. Na przykład budynek Texas Capitol miał taki system zainstalowany w maju 2010 roku; Jednak Teksańczycy noszący ukryte pistolety muszą jedynie okazać swoją licencję, aby móc całkowicie obejść skany. Nowsze maszyny z portalami śledzenia mogą również wykrywać wiele materiałów wybuchowych. Osoba wchodząca musi stać nieruchomo przez kilka sekund, podczas gdy urządzenie uwalnia kilka podmuchów powietrza i pobiera próbki, które są następnie analizowane pod kątem szeregu substancji niebezpiecznych lub wybuchowych. Kiedy strażnik nie jest obecny, komputerowy głos nakazuje osobie iść dalej lub kołowrót może przytrzymać osobę w miejscu. Takie urządzenia mogą być odpowiednie dla wszystkich, którzy wchodzą do pomieszczeń wymagających bardzo wysokiego poziomu bezpieczeństwa, a także przy wejściach do obszarów krytycznych lub pomieszczeń sprzętowych. W styczniu 2013 r. Administracja Bezpieczeństwa

Transportu (TSA) ogłosiła, że 200 określonych skanerów całego ciała zostanie usuniętych z lotnisk w Stanach Zjednoczonych z powodu obaw dotyczących rozdzielczości nagich obrazów produkowanych przez maszyny Rapiscan TM. W grudniu 2012 r. DHS ogłosił, że zleci Narodowej Akademii Nauk dokładne badanie natężenia promieniowania elektromagnetycznego w skanerach bezpieczeństwa.

Mechanizm obejściowy

Niezależnie od zastosowanych systemów powinien istnieć jeden klucz obejściowy, który może otworzyć wszystkie drzwi z elektronicznym lub elektrycznym sterowaniem. Klucz obejścia służy wyłącznie do użytku awaryjnego. Jest to unikalny klucz, którego nie ma w żadnym systemie masteringu i jest dostępny tylko dla kilku zaufanych osób. Cylindry powinny być ciężkie i bardzo trudne do pokonania, a klucze prawie niemożliwe do skopiowania. Niezbędna jest staranna kontrola i ochrona każdego klucza. Utrata klucza może nie zostać szybko wykryta, a czas i koszty ponownego wprowadzenia klucza będą znaczne. Tymczasem każde drzwi w systemie kontroli dostępu są narażone na ataki.

Może być również potrzebne obejście haseł dla indywidualnych użytkowników. Hasła te powinny wywoływać cichy alarm za każdym razem, gdy są używane, aby ochrona mogła odpowiedzieć na witrynę lub zweryfikować tożsamość przez telefon, nadzór lub domofon. Hasła jednorazowe zapewniają najlepsze bezpieczeństwo.

Alarmy włamaniowe

Alarmy włamaniowe są niezbędne do zapewnienia alarmów obwodowych i wczesnego ostrzegania i są zwykle potrzebne jako dodatkowe warstwy bezpieczeństwa. Istnieje kilka metod wykrywania włamań. Cyfrowe kamery monitorujące z detekcją ruchu są najlepsze, ponieważ mogą wizualnie monitorować, co się dzieje i nagrywać to, co widzą. Inne metody obejmują czujniki zbliżeniowe i ciśnienia zamontowane w ścianach obwodowych lub podłogach lub dyskretnie w pomieszczeniu. Większość z tych czujników może wykryć wtargnięcie i włamanie i mogą wskazać lokalizację problemu, ale nie zapewniają żadnych szczegółów, monitorowania ani możliwości rejestrowania dowodów. Czujniki zbliżeniowe i ciśnienia mogą niedrogo chronić obwody na duże odległości, trasy kablowe i media. Koncentryczne warstwy takich urządzeń są niezbędne do dostatecznego wczesnego ostrzegania, aby zapobiec wystąpieniu problemów. Najlepsze czujniki ruchu wykorzystują kamery monitorujące z wykorzystaniem cyfrowej telewizji przemysłowej (CCTV), które mogą wykrywać ruch podczas obserwacji i nagrywania zdarzenia. Miniaturowe kamery, które są niepozorne lub ukryte, są szczególnie skuteczne i coraz tańsze. Kilka kamer może rejestrować obrazy pod różnymi kątami i często może pozytywnie zidentyfikować intruza. Na większym obszarze kamery często używają obrotowo-odchylanych uchwytów i obiektywów zmiennoogniskowych, którymi można sterować również automatycznie i zdalnie. Preferowane są kamery kolorowe, podobnie jak kamery, które automatycznie dostosowują się do warunków oświetleniowych, w tym do prawie ciemności. Niektóre kamery CCTV zawierają wojskowy tryb nocny, który jest względnie niedrogi i dobrze funkcjonujący w prawie całkowitej ciemności. Kamery te działają również dobrze w normalnym świetle i mogą automatycznie przełączać się w tryb nocny, gdy jest to konieczne, aby widzieć wyraźnie i rejestrować dowody. Inne typy kamer, takie jak podczerwień, działają dobrze tam, gdzie nie ma (ludzkiego) światła widzialnego. Inne detektory wtargnięcia wykorzystują technologię radarową lub mierzą zmiany pojemności lub indukcyjności w celu wykrycia wtargnięcia. Większość kamer i detektorów może wyzwolić alarm, gdy tylko zostaną wyłączone lub utracą zasilanie. Detektory mogą być urządzeniami montowanymi na ścianie lub suficie jako jawny środek odstraszający, ale mogą być wtedy podatne na natryskiwanie farby, przecinaków do drutu, pistoletu lub pałki. Dlatego czujniki wykrywania włamań są zwykle ukryte lub co najmniej niepozorne. Alarmy obwodowe są szczególnie ważne w obszarach głównych budynków

lub w obszarach publicznych wewnątrz lub na zewnątrz budynku, aby zapewnić wystarczające wczesne ostrzeżenie o włamaniu, które może wkrótce mieć wpływ na bezpieczny obszar. Cyfrowe kamery wideo są do tego najlepsze, ale mogą być nieskuteczne na dużych obszarach lub na duże odległości. Dlatego do monitorowania włamań używa się wielu urządzeń zbliżeniowych. Większość z nich wykorzystuje długie przewody czujnika, które są dyskretnie montowane powierzchniowo lub ukryte w ścianach działowych, sufitach, a czasami wewnątrz rur. Systemy te wykrywają obecność stojącego dorosłego lub dużego zwierzęcia, które może znaleźć się w odległości kilku stóp od przewodu czujnika. Przewody czujnika mogą być bardzo długie, dlatego często konieczne jest wyznaczenie stref, aby zlokalizować incydent przynajmniej w ogólnej lokalizacji. Lepszą i tańszą alternatywą mogą być światłowodowe alarmy obwodowe. Opracowane dla wojskowych i narodowych instalacji bezpieczeństwa systemy światłowodowe są bardzo czułe i mogą monitorować, oceniać i rejestrować zdarzenia. Przewody czujnika mogą być również osadzone w ścianach działowych z płyt kartonowo-gipsowych lub murowanych, sufitach, podłogach lub kanałach i będą wykrywać zarówno zmiany ciśnienia, jak i dźwięki otoczenia. Ponieważ nie mierzą bliskości i mogą monitorować i oceniać zdarzenia, fałszywe alarmy są mniej prawdopodobne. Mogą ostrzec o zbliżającym się wypadku lub próbach włamania, a wkrótce mogą również zlokalizować wydarzenie. Systemy te używają oprogramowania, które może rozróżniać rozpoznane zdarzenia i sytuacje, które są nieznane lub potencjalnie niebezpieczne. Wszystkie zdarzenia są rejestrowane i mogą być w dowolnym momencie odtwarzane i przeglądane przez zdalnego operatora. Coraz częściej dostępne są niedrogie monitory, które łączą się bezprzewodowo przez Wi-Fi, sieci kratowe, telefon komórkowy, satelitę, kanał radiowy lub czasami przez kuchenkę mikrofalową. Takie urządzenia oszczędzają wysokie koszty bezpośredniego okablowania do odległych obszarów oraz konieczność ochrony i ukrycia okablowania. Ale jest też kompromis z niezawodnością i bezpieczeństwem, ponieważ każde urządzenie o częstotliwości radiowej może być monitorowane lub zagłuszane, a także może zostać sfałszowane. Oprócz alarmów włamaniowych należy zapewnić alarmy środowiskowe do pomiaru temperatury, wilgotności, dymu, pożaru i powodzi we wszystkich krytycznych obszarach i szafach sprzętowych

Inne ważne alarmy

W większości krytycznych obszarów zalecany jest system sygnalizacji przymusu. Zwykle jest to duży czerwony przycisk lub w widoczny sposób zamontowany przy wyjściu interkom awaryjny. Jest używany, gdy ktoś jest ranny lub chory, gdy pojawiają się kłopoty, których inne alarmy nie są od razu wyczuwalne lub gdy grozi przemoc. Typy interkomów awaryjnych są najlepsze, ponieważ każda ze stron może rozmawiać i słuchać. Te z kamerą CCTV są opisane tutaj, ale wiele niedrogich interkomów awaryjnych, które zapewniają tylko dźwięk, może być przydatnych. Pracownicy ochrony mogą stale monitorować wszystkie dźwięki w bezpiecznym obszarze, a każdy znajdujący się wewnątrz może z łatwością porozmawiać z personelem ochrony. Alarmy pod przymusem są zwykle ciche. A urządzenia aktywujące mogą być ukryte lub zlokalizowane w sposób dyskretny na wypadek potencjalnie gwałtownej sytuacji. Aktywatory alarmu przymusu wewnątrz szuflad kasowych, w kolanach biurek lub pod ladami są powszechne od lat. Inną formę alarmu przymusu można zintegrować z systemami dostępu do kart lub systemami haseł, na przykład przesunięcie karty do tyłu może umożliwić dostęp, ale także po cichu wyzwolić alarm na stacjach ochrony. Karty zbliżeniowe można zaprogramować tak, aby rozpoznawały specyficzne metody machania kartami, które mogą przejść kontrolę osób stosujących przymus, a jednocześnie zainicjować odpowiednią obronę i alarmy. Wprowadzenie kodu z dodatkową sekwencją może zrobić to samo. Wszystkie takie sygnały alarmu przymusu powinny być częścią szkolenia każdego pracownika w zakresie korzystania z systemów bezpieczeństwa. Poza kontrolą dostępu i uwierzytelnianiem ważne jest również, aby wiedzieć, kiedy zamknięte drzwi nie są całkowicie zamknięte. Powinien być zainstalowany czujnik ostrzegający o otwarciu lub uchyleniu drzwi z kontrolą dostępu. Czujnik jest zwykle wbudowany w ościeżnicę (ościeżnicę) drzwi, aby zapewnić cichy

alarm. System alarmowy otwartych drzwi opóźnia się o kilka sekund, aby jedna upoważniona osoba mogła normalnie wejść lub wyjść. Krótkie opóźnienie zapobiega pozostawieniu uchylonych drzwi, aby ktoś inny mógł je otworzyć, zaczepianiu się, gdy inna osoba wchodzi lub wychodzi, i ma tendencję do zapobiegania włożeniu lub wyjęciu dużych przedmiotów. Alarm otwartych drzwi zapobiega również podparciu drzwi w dowolnym momencie. Czujniki otwarcia drzwi powinny być przez cały czas ukryte, aby użytkownicy nie byli świadomi ich istnienia. W przeciwnym razie mogą zostać nagrani, zakleszczeni lub w inny sposób pokonani. Ostatnim zabezpieczeniem jest zapobieganie podwójnemu zanurzeniu, w którym upoważniona osoba żąda wielokrotnych wejść w celu wpuszczenia osób nieupoważnionych. System kontroli dostępu może temu zapobiec; gdy osoby wejdą na miejsce, muszą zostać wylogowane, zanim będą mogły ponownie wejść.

SYSTEMY NADZORU

Obecnie systemy nadzoru są projektowane i rozplanowane tak, aby w pełni dokumentować każde zdarzenie, ułatwiać pozytywną identyfikację osobistą oraz dostarczać dowodów prawnych w razie potrzeby. Dzisiejsze cyfrowe aparaty fotograficzne, kontrolery i rejestratory potrafią to wszystko i wiele więcej. Stare kamery i rejestratory analogowe lub filmowe są nieodpowiednie i należy je wymienić, zwłaszcza że nowe systemy monitoringu są znacznie tańsze. Jeśli ochrona jest dobrze zaprojektowana, kamery mogą zapewnić niezaprzeczalny, dokładny, historyczny zapis, który jest dostępny natychmiast. Kamery nigdy nie zasypiają i nie rozpraszają ich powtarzające się czynności lub nuda. Co ważniejsze, kamery mogą zapewniać wczesne ostrzeżenie i dokumentować zdarzenia z wielu perspektyw, jednocześnie i synchronicznie. Kamery coraz częściej zawierają mikrofony i interfejs z awaryjnymi interkomami audio, aby lepiej ocenić sytuację, pomóc ludziom na miejscu zdarzenia lub wyzywać podejrzane osoby. Sama obecność widocznych, ale niedostępnych kamer zwykle odstrasza większość wichrzycieli. Ochrona infrastruktury wymaga zarówno wczesnego ostrzegania, jak i określenia charakteru problemu, zanim do niego dojdzie. Systemy nadzoru wiadomości mogą to robić skutecznie. Można je również zintegrować z innymi alarmami i systemami bezpieczeństwa obiektów, aby zapewnić silną, bezproblemową ochronę.

Kamery nadzoru

Kamery monitorujące są znacznie skuteczniejsze i znacznie tańsze niż strażnicy, strażnicy czy dodatkowe recepcjonistki. Jednak w celu zapewnienia silnej, nadmiarowej i elastycznej ochrony w ważnych lokalizacjach potrzebne będą zarówno kamery, jak i ludzie. Możliwości nadzoru stają się coraz skuteczniejszymi urządzeniami ochronnymi. Teraz mogą zobaczyć więcej, wykryć niebezpieczne ukryte materiały i coraz częściej zdecydować, co jest ważne do monitorowania. Pomieszczenia sprzętowe i inne wrażliwe obszary kiedyś opierały się na czujnikach ruchu w celu zapewnienia bezpieczeństwa, ale teraz kamery cyfrowe z wykrywaniem ruchu działają lepiej. Aparaty cyfrowe działają również dobrze w pomieszczeniach i na zewnątrz, w większości warunków oświetleniowych, od światła słonecznego wpadającego do obiektywu po prawie, jeśli nie całkowitą ciemność. W przypadku stosowania na zewnątrz aparaty cyfrowe są odporne na wszystkie warunki pogodowe oprócz bardzo trudnych. Są jednak narażeni na ciężki dym, śnieg, lód i deszcz. Obiekty zdmuchiwane przez wiatr, a czasami ptaki lub małe zwierzęta mogą rozpraszać ich systemy wykrywania ruchu. Dzisiejsze systemy cyfrowe są znacznie bardziej wydajne i niezawodne niż wcześniejsze aparaty analogowe czy na film. Kamery były kiedyś słabym ogniwem, ponieważ szczegóły nie były jasne lub zbyt małe. Wiele starych aparatów było potrzebnych do pokrycia obszaru, a nawet wtedy niezbędne szczegóły były często nieostre. Teraz aparaty są znacznie mniejsze, tańsze i wykorzystują funkcje automatycznego ustawiania ostrości, pochylenia i zoomu, aby uzyskać znacznie lepsze zdjęcia. Prawie wszystkie kamery używają teraz również koloru dla lepszej przejrzystości. Niektóre zawierają również niedrogi, monochromatyczny tryb noktowizora, który działa dobrze w całkowitej ciemności. Aparaty cyfrowe automatycznie

korygują elektronicznie i mechanicznie zmienne warunki oświetlenia otoczenia. Większość z nich może korygować warunki oświetlenia tła, które w przeciwnym razie powodowałyby niedoświetlenie obiektów, światło słoneczne wpadające bezpośrednio w obiektyw oraz niezwykłą jasność, która w przeciwnym razie zmyłaby użyteczny obraz. Wszystkie obrazy można oglądać w czasie rzeczywistym, a jedna lub więcej osób może jednocześnie kontrolować widoki i przewijać wstecz, aby zamrażać i powiększać klatki. Wszyscy widzowie mogą regulować jasność, kontrast, kolory i powiększenie, a także stosować filtry, aby wydobyć zamglone szczegóły. Każdy przeglądający może zapisać wszystko, co obejrzał. Wszystkie oprócz najmniejszych kamer wewnętrznych są teraz wyposażone w mikrofon, dzięki czemu rejestrowane są zarówno wideo, jak i audio. Poza obiektami niektóre instalacje łączą się z sytuacją awaryjną przez interkom, dzięki czemu dźwięk w tle jest stale monitorowany i nagrywane dialogi. Domofony w nagłych wypadkach są szczególnie dobrym środkiem odstraszającym, ponieważ pracownicy ochrony mogą stawić czoła potencjalnym wichrzycielom i poinformować ich, że są nagrywani. Większość wycofa się lub ucieknie, zanim pojawią się kłopoty. Chociaż wiele systemów sterowania kamerami ma zapewniać zoom elektroniczny, podstawowa funkcja zoomu powinna być mechaniczna. Elektroniczne systemy zoom są niedrogie, ale tracą rozdzielczość, a obrazy mogą szybko stać się niezidentyfikowane. Miniaturowe kamery mogą być szczególnie przydatne, a także oszczędzać pieniądze. Kamery o średnicy mniejszej niż jeden cal mogą zapewnić ostre szczegóły. Niektóre jednostki z obiektywami zmiennoogniskowymi i uchwytami obrotowymi i pochylanymi mogą być ukryte w każdym typowym obiekcie. Istnieją różne opinie co do etyki używania ukrytych kamer, a niektóre przepisy stanowe ograniczają ich użycie jako naruszenia prywatności. Ogólnie zasady dobrej praktyki nadzoru są takie same, jak w przypadku monitorowania rozmów telefonicznych, poczty elektronicznej i korzystania z Internetu. Aby się chronić, organizacja ma prawo widzieć i słyszeć, co dzieje się na jej terenie i wokół niej. Należy jednak umieścić znaki tak, aby pracownicy i ludność byli poinformowani, że wszystkie osoby wchodzące na teren obiektu mogą być monitorowane ze względów bezpieczeństwa. Polityka firmy powinna to wyjaśniać i dlaczego nadzór jest konieczny.

Lokalizacje i mocowania kamer

Aby odstraszać, niektóre kamery powinny być dobrze widoczne, ale może to powodować pewne problemy. Kamery umieszczone zbyt wysoko nie nadają się do identyfikacji ludzi, podczas gdy kamery umieszczone zbyt nisko mogą zostać pomalowane, zakryte lub rozbite. Każda widoczna kamera może zostać wystrzelona (być może niezauważona za pomocą tłumika). Starsze kamery nadają się do użytku jawnego, ponieważ są duże i mogą zapewniać zapasowy nadzór. Inną opcją są atrapy kamer, z których niektóre mają widoczne lampki kontrolne lub automatycznie przesuwają się, aby przyciągnąć uwagę. Niektóre atrapy kamer są w rzeczywistości alarmami, które włączą się, jeśli urządzenie zostanie zakłócone lub jeśli jego przewody zostaną przecięte. Nadzór nad rozległym obszarem wymaga umieszczonej na podwyższeniu kamery, która może widzieć większe odległości, przybliżać szczegóły (zwłaszcza twarze i tablice rejestracyjne pojazdów) oraz uważnie śledzić wydarzenie. Widoki rozległe są również konieczne, aby dostrzec wielu wichrzycieli. Aby zebrać dobre dowody, prawdopodobnie będzie potrzeba kilku ujęć kamery. Kamery zewnętrzne są zwykle mocowane do obrotowego, pochylanego uchwytu i wewnątrz odpornych na warunki atmosferyczne kopułek lub większych obudów, gdy potrzebne są duże obiektywy zmiennoogniskowe. Zwykle nie ma próby ukrycia się, ponieważ kamery są zbyt wysoko, aby sięgnąć, a także zapewniają dobre odstraszanie. Wiele z nich może być jednak niepozornych lub nawet zamaskowanych. Gdy używane są duże kamery i obudowy, kierunek, w którym patrzy kamera, może być oczywisty. Często wichrzyciele odwracają uwagę, aby odciągnąć kamery od prawdziwych problemów.

Systemy rejestrujące

Kiedyś magnetowidy były normą, ale obecnie większość nagrań odbywa się za pomocą dysków twardych, które mogą przechowywać setki godzin dźwięku i obrazu pobranego z wielu źródeł. Coraz częściej używane są również dyski półprzewodnikowe. Kiedyś tylko jedna osoba mogła przeglądać taśmy, a potem zwykle dopiero po zakończeniu nagrywania. Teraz jedna lub więcej osób może mieć dostęp do informacji i analizować je jednocześnie. Kiedyś rekomendowano 31 taśm VCR dla każdego systemu: jedna taśma na każdy dzień miesiąca, po czym taśma była sprawdzana i ponownie używana. Teraz jeden dysk twardy może nagrywać dane z miesiąca, które można następnie niedrogo zarchiwizować na dyskach DVD lub w zdalnych miejscach przechowywania. Magnetowidy często nagrywały w trybie poklatkowym, aby oszczędzać taśmę, aż do wystąpienia zdarzenia wyzwalającego nagrywanie w czasie rzeczywistym. Teraz wszystko może być rejestrowane w sposób ciągły w czasie rzeczywistym, aby w pełni zbadać wydarzenia przed, w trakcie i po wydarzeniu.

Camera Control

Systemy sterowania kamerami

Systemy sterowania kamerami zwykle mogą kierować obrotem (panoramą), pochyleniem, zoomem mechanicznym, przysłoną i oświetleniem tła każdej kamery. Niektóre systemy sterowania mogą automatycznie przesuwać kamery w przód i w tył na dużych obszarach widzenia, a także zapewniają wykrywanie ruchu. Niektóre systemy sterowania mogą również przestać przesuwać i przybliżać nietypowe zdarzenia. Jest to cenna funkcja, którą należy starannie zaprogramować, aby system nie był rozpraszany przez fałszywe zdarzenia lub celowe zmiany. Zwykle każdą kamerą można również sterować ręcznie, często z odległych lokalizacji. Główną zaletą systemu cyfrowego jest to, że każda kamera zapewnia ciągły obraz, zwykle z prędkością około 30 klatek na sekundę, który światłowód i inne połączenia szerokopasmowe wprowadzają do systemu nagrywania w czasie rzeczywistym i w wysokiej rozdzielczości. Systemy sterowania zwykle pozwalają jednej lub kilku osobom cofnąć obrazy bez wpływu na nagrywanie w czasie rzeczywistym. Każda przeglądarka może przewijać do tyłu i do przodu, zamrażać klatki, powiększać, przycinać lub ulepszać obraz elektronicznie i zapisywać dowolny materiał w innym medium lub system jako dowód.

Połączenia szerokopasmowe

Zaletą szerokopasmowych połączeń kamer jest to, że informacje są dostępne w czasie rzeczywistym i w wysokiej rozdzielczości, a także to, że dostępnych jest więcej funkcji sterowania kamerą. Okablowanie światłowodowe robi to najlepiej, ale powinno być dedykowane i dobrze chronione. Kamery zdalne można również podłączać za pośrednictwem sieci LAN, bezprzewodowego lub szerokopasmowego połączenia internetowego przy użyciu protokołu kontroli transmisji / protokołu internetowego (TCP / IP), jeśli zostanie to wykonane ostrożnie, aby dane były bezpieczne, a inny ruch nie był utrudniony. Cyfrowe multipleksowanie to kolejna zaleta połączeń szerokopasmowych. Kiedyś multipleksowanie przez metalowe okablowanie wymagało opóźnień, niższej rozdzielczości i mniejszej liczby klatek przesyłanych na sekundę, mimo że każda kamera zapewniała ciągłe obrazy o wysokiej jakości. Teraz cyfrowe multipleksowanie przez połączenia światłowodowe umożliwia jednoczesne przesyłanie wszystkich danych ze wszystkich kamer. Multipleksowanie odbywa się zdalnie, ponieważ sygnały z kilku kamer są łączone w jedno szerokopasmowe połączenie z systemem sterowania. Połączenia między systemami sterowania są również multipleksowane, aby zminimalizować opłaty za łącza. Interfejsami sygnałowymi między każdą kamerą a multiplekserem mogą być światłowody, mikrofale, sieć lub Internet. W ten sposób setki kamer można tanio połączyć w sieć. Kolejną zaletą dzisiejszych połączeń TCP / IP dla kamer jest to, że mogą być one połączone z Internetem, co umożliwia stacjom monitorującym odbieranie danych bez konieczności modernizacji specjalnych kabli w całej konstrukcji. Wadą takich systemów jest to, że są one w związku z tym podatne na te same metody

ataków, które zostały opracowane w celu hakowania innych systemów internetowych. Właściwe użycie szyfrowania (np. Wirtualnych sieci prywatnych) dla wyjścia kamery i sterowania może pomóc w ochronie systemów nadzoru przed manipulacjami elektronicznymi. Szyfrowanie może również kolidować z atakami odtwarzania, tak popularnymi w filmach, w których przestępcy wkładają urządzenia, aby wywołać nieskończoną pętlę odtwarzania i oszukać obserwatorów, którzy uwierzyli, że w zagrożonych strefach nadzoru wszystko jest w porządku. Dodatkowe informacje na temat technik penetracji. Multipleksowanie radiowe lub mikrofalowe jest inną opcją, ale nie jest zbyt szybkie i podlega zakłóceniom lub zakłóceniom podczas trudnych warunków pogodowych.

PROJEKTOWANIE OBIEKTÓW

Dobra ochrona zaczyna się od dobrego projektu obiektu, który zapewni bezpieczeństwo infrastruktury informatycznej i korzystających z niej ludzi. Systemy ochronne stają się drogie i nieefektywne, gdy same pomieszczenia nie zapewniają dobrego zabezpieczenia. Odpowiedni projekt wnętrz, rozplanowanie obiektów, inżynieria i konstrukcja mogą zmaksymalizować skuteczność zabezpieczeń, zminimalizować koszty, zwiększyć produktywność i morale oraz ogólnie zwiększyć zyski. Punktem wyjścia jest inspekcja wszystkich lokalizacji i przegląd wszystkich planów powykonawczych i dokumentów budowlanych. Inspekcje i przeglądy bezpieczeństwa pomieszczeń najlepiej usprawnić przy pomocy niezależnych, zewnętrznych ekspertów ds. bezpieczeństwa. Kompleksowe i obiektywne doświadczenie w architekturze, projektowaniu, inżynierii, infrastrukturze IS i bezpieczeństwie pomieszczeń jest potrzebne i nie wszystkie mogą być dostępne wewnętrznie lub od dostawców. Proces inspekcji i przeglądu zawsze musi odnosić się do konkretnego zagrożenia i musi odnosić się do dokładnej oceny zagrożenia. Inspekcja lokalu może następnie służyć do weryfikacji luk w zabezpieczeniach zidentyfikowanych w ramach oceny zagrożenia. Po naprawieniu niektórych luk należy powtórzyć inspekcję lokalu. Skuteczna ochrona infrastruktury może zapobiec występowaniu problemów. Aby to zrobić, konieczne jest dostateczne wczesne ostrzeganie, które z kolei wymaga dobrego planowania i projektowania obiektów, efektywnego zabezpieczenia pomieszczeń i infrastruktury oraz świadomości i czujności wszystkich w okolicy. Wszyscy muszą ze sobą współpracować bezproblemowo, wydajnie i proaktywnie. Dobry projekt obiektów może być wydajny, nieinwazyjny, opłacalny i niedrogi - nawet w istniejących obiektach. Oto kilka wskazówek i sugestii.

Wybór bezpiecznych witryn

Jeśli to możliwe, plac budowy dowolnego obiektu, w którym będzie znajdować się infrastruktura IS - szczególnie w przypadku wysoce bezpiecznych zastosowań - powinien być daleki od oczywistych zagrożeń ze strony człowieka, takich jak składy paliw, linie kolejowe, mosty wiszące, wiadukty na autostradach dużych prędkości i trasy przelotów na lotniska. Miejsca powinny unikać oczywistych zagrożeń naturalnych, takich jak tereny zalewowe, obszary narażone na pożary lasów, aktywne wulkany i stare podziemne kopalnie, w przypadku których następuje zapadanie się obszarów leżących. Dostęp do miejsca powinien obejmować możliwość ewakuacji pracowników i gości w nagłych wypadkach oraz możliwość dotarcia do obiektu pojazdów ratowniczych, nawet jeśli główny dostęp publiczny jest zablokowany. W miastach budynek nie powinien znajdować się w dzielnicach o wysokiej przestępczości lub w parkach przemysłowych z niewystarczającym nadzorem bezpieczeństwa lub historią kradzieży, wandalizmu lub sabotażu. Decyzje powinny uwzględniać publiczne rejestry wskazujące wystarczająco kompetentne zespoły policji i straży pożarnej; W podjęciu decyzji o ostatecznym wyborze lokalizacji pomocne mogą być wywiady z innymi użytkownikami obiektów przemysłowych lub handlowych w okolicy. Miejsca na pomieszczenia sprzętowe i pomieszczenia gospodarcze powinny być chronione przed możliwymi zagrożeniami. Miejsca infrastruktury powinny być zlokalizowane z dala od wszelkich rurociągów, zbiorników lub urządzeń wykorzystujących jakąkolwiek ciecz, która mogłaby wyciekać lub rozlać się. Większość instalacji wodociągowych ma

tendencję do nieoczekiwanego wycieku w pewnym momencie lub może zostać celowo przerwana, więc dobrze jest założyć, że jakakolwiek rura, połączenie, pojemnik lub pompa w końcu pękną lub wycieknąą. Umieszczanie wrażliwych witryn z dala od takich zagrożeń jest bezpieczniejsze i tańsze niż jakakolwiek inna forma ochrony. Strefa niebezpieczna, w której mogą się rozprzestrzeniać wycieki, musi obejmować dużą odległość w pionie i obszar poziomy. Strefę niebezpieczną należy rozpocząć od piramidy z dowolnego źródła wycieku, w dół o kilka pięter i na zewnątrz poziomo, daleko poza obszarami infrastruktury. Większość budynków wymaga tryskaczy przeciwpożarowych we wszystkich obszarach. Każdy może zostać uruchomiony przez przypadek, akt wandalizmu lub rzeczywisty pożar i może spowodować znaczne zalanie. Ponadto miejsca infrastruktury powinny być zlokalizowane z dala od okien, ścian zewnętrznych, dachów, świetlików, przeszkód budowlanych i kanalizacji burzowej, które są potencjalnymi źródłami powodzi. Uzdatniana woda używana do ogrzewania, klimatyzacji i systemów solarnych stanowi gorszy problem, ponieważ chemikalia mogą szybko zniszczyć sprzęt elektroniczny, złącza i okablowanie. Jeśli cała infrastruktura nie może być umieszczona w bezpiecznej odległości od wszelkich płynów i materiałów niebezpiecznych, muszą istnieć specjalne zabezpieczenia i alarmy. Zabezpieczenia obejmują uszczelnioną, wodoodporną konstrukcję, odpływy, nasypy lub inne urządzenia odwracające ruch, a także odpowiednie materiały pod ręką, aby kontrolować wszelkie wycieki. W pobliżu miejsc, w których mogą wystąpić wycieki lub wycieki, powinny znajdować się czujniki alarmu środowiskowego. Odpływy podłogowe muszą również chronić obszary wyposażenia, zwłaszcza te, w których są używane tryskacze; w przeciwnym razie czyszczenie będzie trudne. Miejsca infrastruktury nie powinny być widoczne ani dostępne z żadnego obszaru publicznego. Okablowanie lub kable infrastruktury nie powinny przebiegać przez rdzeń budynku, obszary publiczne ani mechaniczne, w tym toalety, zlewy, toalety i klatki schodowe. Unikaj umieszczania sprzętu lub kabli w miejscach, w których mogą się kroczyć osoby. Wszystkie wejścia do pomieszczeń technicznych powinny być dobrze widoczne z miejsc pracy, aby pracownicy mogli z łatwością obserwować wszystkie wejścia i wyjścia. Wybór z natury bezpiecznych miejsc i wejść znacznie zmniejsza zarówno ryzyko, jak i koszty, ponieważ potrzebne jest mniejsze bezpieczeństwo. Aby zapewnić skuteczną kontrolę bezpieczeństwa, powinien istnieć tylko jeden punkt dostępu do każdego obszaru krytycznego, używany zarówno do wejścia, jak i do wyjścia. Jeśli jednak lokalne przepisy przeciwpożarowe lub budowlane wymagają drugorzędnych środków ewakuacyjnych, zwykle dopuszczalna jest listwa antypaniczna z opóźnionym dostępem. Taki system opóźnia zwolnienie blokady wyjścia na kilka sekund, podczas gdy włącza się alarm i zostaje uruchomiona kamera monitorująca. We wszystkich chronionych obszarach powinny być również zainstalowane kamery monitorujące z wykrywaniem ruchu. Wszystkie zamknięte drzwi powinny wyglądać jak najbardziej do siebie podobne z zewnątrz i być identyfikowane tylko przez numer pokoju, który wygląda podobnie do wszystkich innych drzwi do lokalu. Żadne imię i nazwisko ani stanowisko osoby, ani żaden inny sposób identyfikacji tego, co znajduje się w zamkniętym obszarze, nie powinny być widoczne. Żadne oznakowanie ani katalog nie powinny zawierać nazwy funkcjonalnej, osobistej ani działu, ale w razie potrzeby tylko numery obszarów lub pomieszczeń i strzałki kierunkowe. Tylko numery pięter, pokoi lub lokali powinny pojawiać się na znakach lokali, na piętrach.

Dostęp fizyczny

Dostęp do terenu zakładu powinien być kontrolowany. Strażnicy przy wejściu nie zatrzymają terrorystów, ale mogą zapewnić wczesne ostrzeżenie o kłopotach. Wszystkie takie stacje powinny być pod stałym nadzorem i mieć zainstalowane przyciski napadowe służące do powiadamiania służb ochrony o wystąpieniu problemu przy wejściu na teren zakładu. Pachołki żelbetowe mogą zapobiegać fizycznemu atakowi na budynek, zakłócając nawet szybkie taranowanie zwykłych pojazdów, takich jak samochody osobowe, dostawcze i lekkie ciężarówki. Niekoniecznie będą one zapobiegać atakom z wykorzystaniem przejętych dużych pojazdów, takich jak załadowane wywrotki. Wejścia do budynków nie powinny obejmować dużych przeszklonych ścian, które można by łatwo wyburzyć, aby uzyskać

dostęp do hal wejściowych w celu zdetonowania bomb. Fizyczny dostęp do wszystkich części infrastruktury informatycznej powinien być ograniczony. Cały system informatyczny i sprzęt sieciowy muszą znajdować się w pomieszczeniach sprzętowych, które są zawsze zamknięte i dostępne tylko dla tych, którzy muszą tam być. Wszystkie węzły sanitarne i węzły dystrybucji okablowania, panele dystrybucji zasilania, panele krosowe, bloki okablowania i zakończenia powinny znajdować się wewnątrz pomieszczeń sprzętowych, które są zawsze zamknięte. Jeśli to możliwe, nie wolno wpuszczać niezwiązanych ze sobą systemów, sprzętu lub mediów wewnątrz obszaru o ograniczonym dostępie, aby technik pracujący w niepowiązanym systemie nie mógł uzyskać dostępu do infrastruktury informatycznej. Jeśli nie można tego uniknąć, personel IS powinien zawsze eskortować inne osoby wchodzące do tych obszarów. W obszarach o wysokim poziomie bezpieczeństwa wszystkie wchodzące osoby powinny być eskortowane lub korzystać z dwuosobowych zespołów zaufanych osób, w których każda osoba obserwuje drugą. Strażnicy i pracownicy ochrony obiektów są dobrymi eskortami ochrony, ale prawdopodobnie nie znają infrastruktury i nie są tutaj najlepszym wyborem. Personel IS jest lepszą eskortą, nawet jeśli nie zna wszystkich szczegółów dotyczących bezpieczeństwa. W każdym przypadku wszystkie wchodzące osoby muszą zostać zidentyfikowane, a każda wizyta zarejestrowana. Rozsądne jest umieszczenie krytycznych rozdzielnic elektrycznych w pomieszczeniu sprzętowym, aby były one szybko dostępne i chronione. Jest to również kwestia bezpieczeństwa; osoba pracująca przy sprzęcie lub okablowaniu może łatwo zauważyć, że wyłącznik automatyczny jest wyłączony. W przeciwnym razie rozdzielnice elektryczne powinny być umieszczone wewnątrz zamkniętego obszaru, który nie jest oznaczony z zewnątrz inaczej niż zakodowanym numerem lokalizacji. Panele są często umieszczane w miejscach publicznych w wielu budynkach; muszą być następnie bezpiecznie zamknięte i również zaalarmowane. Zawsze, gdy panel elektryczny kontroluje coś krytycznego, dostęp do obszaru powinien być ograniczony, a pomieszczenie zaalarmowane. Te środki ostrożności ograniczają utratę zasilania krytycznych systemów przez przypadek lub celowo. Jednym z przypadków wykorzystywanych na szkoleniach z zakresu bezpieczeństwa obiektów jest odblokowany panel krosowy odkryty przez eksperta ds. bezpieczeństwa fizycznego na korytarzu publicznym szpitala; dyrektor oddziału intensywnej terapii (OIOM) był przerażony, gdy zdał sobie sprawę, że wyłączniki sterujące sprzętem podtrzymującym życie pacjentów na OIT są otwarte dla każdego dziecka lub złośliwej osoby. Osłona może najlepiej kontrolować dostęp do krytycznych pomieszczeń sprzętowych. Osłona to układ dwudrzwiowy z drzwiami wewnętrznymi, drzwiami zewnętrznymi i krótkim korytarzem pomiędzy nimi. Oba drzwi są zaryglowane; jeden musi zostać zamknięty, zanim drugi będzie mógł się otworzyć. Korytarz jest zwykle zbudowany z nietłukącej się szklanej ścianki o pełnej wysokości (często jednokierunkowej) po jednej lub obu stronach w celu nadzoru. Oba drzwi są zwykle bez okien. A każde drzwi muszą mieć silny system kontroli dostępu. Ale ze względów bezpieczeństwa zewnętrzne drzwi można zwykle otworzyć od wewnątrz korytarza za pomocą alarmu antypanicznego. Zwykle jedna lub więcej kamer monitorujących jest ustawionych tak, aby zidentyfikować każdego wchodzącego lub wychodzącego z osłony. Zdecydowanie zaleca się korzystanie z interkomów awaryjnych w korytarzu osłonowym oraz przy wejściach i wyjściach. Wyraźne przyciski przymusu / pomocy powinny aktywować się cicho, aby personel ochrony mógł monitorować obszar i rozmawiać lub rzucać wyzwanie każdemu, kto nie może prawidłowo przejść. Alarmy najlepiej są ciche, aby nikt pod przymusem nie był dalej zagrożony. Domofony awaryjne często zawierają małe kamery, które są niepozorne lub ukryte, dzięki czemu personel ochrony może zobaczyć, co się dzieje, pomóc, jeśli ktoś jest chory lub w jakiś sposób zostanie uwięziony, i uniknąć problemów związanych z bezpieczeństwem publicznym. Dobrze zaprojektowana mantrapa może być cenna w przypadku wszystkich wejść, z wyjątkiem bardzo uczęszczanych. Mantrapy mogą zwiększać bezpieczeństwo na wiele sposobów i zwykle nie są nachalne. Mogą wykryć przechodzenie na barana, gdy jedna lub więcej dodatkowych osób ściśle podąża za osobą upoważnioną do wejścia. Mantrapy same w sobie nie wykluczają podpartych otwartych drzwi, ale sprawiają, że usuwanie przedmiotów z pomieszczenia jest trudne i ryzykowne. Dziennik kontroli

dostępu i nagrania z monitoringu mogą zidentyfikować sprawców i dostarczyć mocnych dowodów na skazanie osób, które w innym przypadku mogłyby być podejrzanymi lub nieznanymi.

Konstrukcja ochronna

Projekt nowego budynku może ulec poprawie jak i bezpieczeństwo fizyczne.

* Unikaj wrażliwych metod budowlanych, takich jak stosowanie słupów konstrukcyjnych w dużych, otwartych przestrzeniach na parterze; zniszczenie takich kolumn przy użyciu materiałów wybuchowych mogłoby spowodować poważne uszkodzenie integralności strukturalnej budynku.

* Nie zezwalaj architektom na umieszczanie dekoracyjnych wgłębień na zewnątrz budynku; takie pionowe wzory mogą zapewnić środki

* Umieść wszystkie IS w utwardzonym, izolowanym miejscu.

Pomieszczenia sprzętowe wymagają solidnych ścianek działowych zapewniających dobre bezpieczeństwo i wytrzymujących znaczny ciężar okablowania i sprzętu. Ponadto przegrody i ściany muszą pozostać bezpieczne i stabilne podczas każdej aktywności sejsmicznej, takiej jak intensywny ruch drogowy lub huk dźwiękowy, eksplozja lub wstrząsy ziemi. Konieczne może być również wzmocnienie podłóg. Solidne ścianki działowe uniemożliwiają włamanie, co w przeciwnym razie można by osiągnąć za pomocą niewiele więcej niż scyzoryka i pięści. Istniejące ściany, ścianki działowe i podłogi powinny zostać sprawdzone, a wszelkie późniejsze zmiany zatwierdzone przez inżyniera budowlanego. Zastanów się też, co może być potrzebne w przyszłości; późniejsze zmiany mogą być bardzo kosztowne lub po prostu niepraktyczne. Okna z definicji nie są solidnymi przegrodami. Unikaj dopuszczania pracowników niezabezpieczonych do wywierania presji na architektów, aby włączyli duże okna, umożliwiając widoczność i ewentualne wtargnięcie do zabezpieczonych obszarów. Umożliwienie niekontrolowanego wglądu w centra operacyjne może pozwolić przestępcom dowiedzieć się więcej o personelu, procedurach i harmonogramach, niż powinni, poprzez zwykłą obserwację. Drzwi antywłamaniowe również powinny być solidne. Powinny być metalowe, ognioodporne i względnie ciężki i ciężki sprzęt. Staraj się nie zwracać uwagi na kontrolowane drzwi żadnym charakterystycznym wyglądem zewnętrznym. Jeśli wiele zajętych obszarów korzysta z drewnianych drzwi, drzwi antywłamaniowe nie powinny się wyróżniać. Metalowe drzwi i okucia, które wyglądają podobnie do wszystkich innych drzwi. Czasami bezpiecznie wyglądające atrapy drzwi, które nie prowadzą do niczego ważnego, są używane do oszustwa lub jako alarmująca miódka, aby odciągnąć wichrzycieli z bezpiecznych obszarów. Dobrze wykonane ścianki działowe i sufity uszczelnią również dym i zatrzymają dym w przypadku pożaru we wnętrzu. Zaleca się uszczelnienie na obwodzie każdych drzwi, aby zapobiec przedostawaniu się kurzu, zanieczyszczeń i wilgoci oraz zatrzymywać dym. Jeśli to możliwe, okablowanie, które musi przebiegać wewnątrz drzwi, powinno być poprowadzone w zawiasach, tak aby żadne przewody nie były widoczne przez cały czas. Odsłonięte przewody mogą zostać przypadkowo uszkodzone przez przecięcie lub uszkodzone na wiele sposobów. Główni producenci zawiasów mogą dostarczyć specjalne zawiasy, które ukrywają większość okablowania i pasują do innych elementów wyposażenia pomieszczeń. Ścianki działowe są zwykle niepotrzebne, chyba że istnieją specjalne wymagania konstrukcyjne lub bardzo wysokie wymagania bezpieczeństwa. Ścianki działowe z płyt kartonowo-gipsowych z metalowymi kołkami są zwykle wystarczające, ale powinny być wyjątkowo wytrzymałe. Zalecane są ognioodporne płyty gipsowo-kartonowe typu X o grubości przynajmniej trzech czwartych cala. Jeszcze lepiej, użyj podwójnych paneli o grubości pół cala lub pięciu ósmych cali. Istniejące ścianki działowe z płyt kartonowo-gipsowych można z łatwością pokryć podwójnymi panelami, aby zwiększyć bezpieczeństwo i wytrzymałość. Ściany działowe murowane, a często również płyty gipsowo-kartonowe, są zwykle licowane wytrzymałą sklejką przeciwpożarową do mocowania wsporników sprzętu i okablowania. To, czy sklejka jest zamontowana

na dystansach, aby można było poprowadzić okablowanie za nią, jest kwestią preferencji. Zwykle bardziej efektywne jest poprowadzenie wszystkich przewodów odsłoniętych w zabezpieczonym obszarze. Nie używaj sufitu podwieszanego (podwieszanego) w żadnym pomieszczeniu sprzętowym. Sufity podwieszane po prostu zwiększają koszty, utrudniają i zmniejszają objętość pomieszczenia. Przestrzeń nad sufitem podwieszanym stanowi zagrożenie pożarowe, a wszystko w jej wnętrzu, w tym wszelkie odsłonięte kable, musi być ognioodporne, co zwiększa niepotrzebne koszty. Większość przepisów budowlanych wymaga oddzielnych stref wykrywania pożaru i głowic gaszących w każdej komorze, co jest dużym kosztem. Usuń wszelkie podwieszane sufity i uzyskaj więcej użytecznej przestrzeni na kable, lepszą cyrkulację powietrza i łatwiejszą konserwację. Z tych samych powodów unikaj podłóg podniesionych. Są bardzo kosztowne, w większości instalacji niepotrzebne funkcjonalnie i zajmują dodatkową powierzchnię na rampy. Podobnie jak sufity podwieszane, podłogi podniesione tworzą przestrzeń nadsufitową, która wymaga oddzielnych stref wykrywania pożaru i głowic gaszących. Podłogi podniesione zwykle ograniczają wysokość sufitu, ponieważ przestrzeń nie została do tego zaprojektowana, więc pomieszczenie musi zostać powiększone, aby pomieścić wszystko, a często z niewielkimi możliwościami rozbudowy na przyszłość.

Podniesione podłogi szybko stają się pułapkami na kurz, a z czasem zwykle zagraceniem nowych, starych i porzuconych kabli, których nikt nie może rozgryźć. Wiele awarii sprzętu było spowodowanych przegrzaniem spowodowanym przepływem powietrza ograniczonym przez zbyt płytką podłogę podniesioną lub zbyt wiele przeszkadzających kabli. Do doprowadzania powietrza chłodzącego rzadko jest potrzebna komora z podniesioną podłogą. Kanały i rejestry montowane na powierzchni zwykle wykonują swoją pracę lepiej i znacznie taniej oraz są łatwe do czyszczenia i modyfikacji. Całe okablowanie można zwykle skutecznie poprowadzić powyżej i między urządzeniami lub przy użyciu niedrogich korytek kablowych montowanych na ścianach i sufitach. W razie potrzeby wyloty podłogowe mogą uzyskać dostęp do przewodów kanałowych w podłodze, które mogą już istnieć, a nie są używane. W przypadku specjalnych potrzeb kanał można przeprowadzić przez płytę podłogową i wzdłuż sufitu poniżej. Ważne jest, aby całe okablowanie na zewnątrz pomieszczeń sprzętowych było chronione wewnątrz metalowego kanału. Ten kanał nie powinien być cienkościenny ani plastikowy, ale z wytrzymałego, wytrzymałego metalu. Metalowy kanał o grubych ściankach jest mocny, trudniejszy do uszkodzenia lub przerwania, a także zapewnia dobre ekranowanie magnetyczne i elektroniczne. Metalowe kanały kablowe mogą być łatwo i powinny być dobrze uziemione. Uzyskaj porady eksperta, gdzie i jak podłączyć uziemienie, aby uniknąć zakłóceń. Metalowy przewód może również służyć jako czujnik zbliżeniowy ostrzegający, gdy coś znajdzie się zbyt blisko. Przewód alarmowy ukryty w kanale zapewnia wczesne ostrzeżenie o problemach i często może wskazać, gdzie się znajduje. Czasami stosuje się gaz obojętny lub żel, aby zwiększyć ciśnienie w przewodach w celu ochrony przewodów; wskazuje spadek ciśnienia , wyciek lub naruszenie, ale nie wskazuje, gdzie może być. Wszystkie przewody powinny wyglądać podobnie, niezależnie od tego, czy przenoszą zasilanie, dane, czy kontrolują bezpieczeństwo systemu. Chociaż średnica przewodu musi się zmieniać, ogólny wygląd powinien być taki sam. Nie oznaczaj ani nie oznaczaj zewnętrznej strony żadnego kanału z wyjątkiem kodu alfanumerycznego. Kable wewnątrz kanału również nie powinny być oznakowane, z wyjątkiem alfanumerycznych. Ogólnie rzecz biorąc, wszelkie przewody w kanale powinny wychodzić tylko wewnątrz na bezpieczną szafę, pomieszczenie sprzętowe lub skrzynkę połączeniową, w której przewody powinny być oznaczone odpowiednimi kodami, które można odszyfrować za pomocą aktualnych podsumowań elektronicznych, dostępnych tylko za zgodą. Kable danych i okablowanie są delikatne, niezależnie od tego, czy są miedziane, czy światłowodowe. Każde nadmierne ciśnienie, zginanie, rozciąganie, wibracje lub zagniatanie może zmienić przekładnię lub spowodować awarię. Kable światłowodowe są szczególnie delikatne; metalowy przewód jest zwykle najlepszą i najtańszą ochroną. Pozwala to uniknąć specjalnych osłon, które są często uciążliwe i kosztowne. Każde

okablowanie, czy to metalowe, czy światłowodowe, może być nieprawidłowo określone, zainstalowane lub zakończone. Okablowanie lub instalacje niespełniające standardów mogą tymczasowo działać dobrze, ale przyszła awaria jest prawdopodobna, prawdopodobnie trudna do zlokalizowania w szybkim tempie i będzie kosztowna w naprawie. Dlatego ważne jest, aby wszystkie kable zostały przetestowane pod kątem akceptacji i certyfikowane przez niezależnego eksperta, zanim instalator zostanie w pełni opłacony. Krytyczne ciągi kablowe powinny być wyposażone w urządzenia alarmowe od końca do końca, niezależnie od tego, czy kanał przenosi zasilanie, dane czy zabezpieczenia. Istnieje kilka sposobów zaalarmowania ciągu kablowego. Przewody zewnętrzne są często zasilane azotem, aby nie dopuścić do zawilgocenia, lub specjalnym żelem, który zapobiega przedostawaniu się tlenu i wilgoci oraz stabilizuje przewody wewnątrz. Przewody wewnętrzne mogą być pod ciśnieniem i alarmowane w ten sam sposób. Monitorowanie ciśnienia zapewnia alarm w przypadku pojawienia się problemu (w tym uszkodzonych uszczelek, które należy szybko naprawić). System jest skuteczny i zapewnia wczesne ostrzeganie, ale nie da się zlokalizować przerw, a wszelkie przyszłe zmiany okablowania mogą być trudne. Czujniki zbliżeniowe i czułe na nacisk mogą również alarmować całą długość krytycznych kabli. Monitorowany kanał może być bardzo długi i może przebiegać przez obszary, które są trudne do ochrony lub nie zapewniają żadnej ukrycia. Chociaż czujniki nadzoru i włamań mogą chronić najważniejsze obszary, często istnieje duża infrastruktura, którą można chronić jedynie za pomocą przewodów czujników biegnących na całej długości kanału. Mechaniczne czujniki ciśnienia wykryją niezwykłe wibracje, natomiast czujniki zbliżeniowe wskazują zmianę w magnetycznym lub elektronicznym środowisku otaczającym kabel lub kanał. Nowsze systemy wykorzystują czujniki światłowodowe, które monitorują ciśnienie akustyczne. Niektóre z tych systemów są wystarczająco inteligentne, aby odróżnić rutynowe, nieszkodliwe zdarzenia od możliwych problemów, a wiele z nich może również z grubsza określić lokalizację. Czasami sam kanał jest czujnikiem lub do niego jest podłączony zewnętrzny przewód, ale te podejścia są często nieskuteczne.

Korzystanie z alarmów istniejących lokali

Różne kody wymagają, aby miejsca pracy miały widoczne i dźwiękowe alarmy pożarowe. Większość miejsc pracy ma również systemy przywoławcze głosowe, interkom alarmowy, nadzór i systemy bezpieczeństwa pomieszczeń. Wszystkie te urządzenia mogą być efektywnie wykorzystywane do zwiększania i wspierania bezpieczeństwa infrastruktury informatycznej. Alarmy dźwiękowe są używane, gdy osoby na miejscu zdarzenia muszą podjąć natychmiastowe działania, takie jak zamknięcie lub ewakuacja. I odwrotnie, ciche alarmy zapewniają wczesne ostrzeżenie i pozwalają ochronie dyskretnie monitorować miejsce zdarzenia, gromadzić dowody oraz reagować i pomagać w razie potrzeby. Wszystkie te alarmy można zintegrować z systemami ochrony infrastruktury, aby zapewnić lepsze wczesne ostrzeganie i dodatkowe poziomy ochrony. Wszystkie alarmy i ostrzeżenia powinny być przesyłane do centralnego punktu ochrony lub posterunku ochrony. Celem jest dokumentowanie reakcji na incydenty i zarządzanie nimi, szybkie wezwanie pomocy, monitorowanie miejsca zdarzenia, gromadzenie dowodów i wspieranie wszystkich zasobów reagowania. Centralne zarządzanie jest szczególnie potrzebne, gdy zagrożenia występują kaskadowo lub występują liczne zdarzenia, co często się zdarza. Kierownicy ds. Bezpieczeństwa, menedżerowie systemów informatycznych, menedżer ds. Bezpieczeństwa infrastruktury i szefowie kluczowych działów również powinni zostać natychmiast powiadomieni. Niektóre z tych osób mogą znajdować się poza siedzibą firmy lub w odległych lokalizacjach, ale będą musiały skutecznie komunikować się przynajmniej z centrum operacyjnym. Powiadomienia i późniejsza komunikacja powinny być szybkie, prywatne, bezpieczne i rejestrowane w celu udokumentowania zdarzeń. Co najmniej jedno centrum kontroli bezpieczeństwa kopii zapasowych online i centrum operacyjne zapewnia nadmiarowość, wsparcie i pomoc oraz silne zabezpieczenia. Skuteczna metoda ostrzegania obejmująca cały lokal wykorzystuje kody głosowe nadawane przez system przywoławczy. Są one zwykle oparte na skryptach i często

wstępnie nagrane, aby alerty mogły być inicjowane automatycznie, zdalnie lub ręcznie. Szpitale robią to skutecznie dzięki swoim kolorowym kodom, odpowiednikom cichych alarmów, które nie wydają się niezwykłe dla opinii publicznej. Skuteczny system kodów alertów w dużej organizacji wykorzystuje również nazwiska fikcyjnych osób. W mniejszym otoczeniu, takim jak szkoła, gdzie nazwiska wszystkich pracowników są znane, mogą być wysyłane komunikaty ostrzegawcze do osoby, która podejmie nieszkodliwe działanie, które jest rozumiane jako kod ostrzegawczy. Dodatkowe informacje alfanumeryczne w komunikacie mogą określać ogólną lokalizację zdarzenia. Podobnie jak w szpitalu, dobrze jest dodać podobne kody do innych rutynowych celów, tak aby opinia publiczna generalnie wyłączała wszystkie strony. Ten system jest szczególnie przydatny, gdy przemoc jest zagrożona lub wybuchła. Chociaż większość pracowników ochrony ma teraz przenośne radia, może być wiele obszarów pozbawionych zasięgu, a niewielu używa słuchawek, aby inni nie mogli łatwo usłyszeć, co się dzieje. Jednak wszyscy pracownicy ochrony muszą natychmiast wiedzieć, kiedy pojawiają się kłopoty, i muszą być ostrzegani w taki sposób, aby nie podniecać innych. Ponadto każdy w obiekcie musi wiedzieć, kiedy grozi sytuacja awaryjna. Rzeczywiście, każdy ma prawo wiedzieć i szybko otrzymać instrukcje dla własnego bezpieczeństwa. Cokolwiek poza tym spowoduje znaczną odpowiedzialność. Dlatego skuteczne procedury, jasne proste instrukcje, dobre przygotowanie i okresowe szkolenia mogą chronić każdego i zapewnić silne bezpieczeństwo. Powszechna dostępność telefonów komórkowych dodała kolejny kanał powiadamiania o zagrożeniach. Pracownicy mogą być powiadamiani o nagłych wypadkach za pomocą krótkich wiadomości tekstowych (SMS). Korzystając z wiadomości generowanych przez komputer, a nawet wiadomości ręcznych, pracownicy ochrony mogą szybko i łatwo dotrzeć do wielu osób zaangażowanych w reagowanie na sytuacje awaryjne. Jeśli telefony są skonfigurowane do używania charakterystycznego tonu dla takich wiadomości i jeśli telefony nie są zwykle używane do swobodnego wysyłania wiadomości, takie ustawienia mogą być przydatne jako uzupełnienie innych metod powiadamiania.

Czysta energia elektryczna

Ochrona sprzętu elektronicznego wymaga źródła energii elektrycznej, które jest stale czyste. Czysta moc zwykle oznacza prąd przemienny o ściśle ograniczonych wahaniach amplitudy i kształtu fali. Przerwy w dostawie prądu i spadki napięcia (stany niskiego napięcia) mogą powodować oczywiste problemy, ale liczne inne zakłócenia mogą zakłócać lub uszkadzać infrastrukturę informatyczną. Niektóre z nich obejmują zapady i zapady, skoki, stany nieustalone oraz zakłócenia magnetyczne lub o częstotliwości radiowej. Większość z nich ma charakter przerywany i niekoniecznie występuje podczas testowania obwodu. Zrozumienie każdego terminu nie jest tak ważne, jak wiedza, że w liniach elektroenergetycznych często występują różnorodne problemy, losowo i bez ostrzeżenia. Szczególnie szkodliwe są przepięcia. Są to obniżenia napięcia przez zakład energetyczny, które mogą spowodować nieprawidłowe działanie lub wyłączenie urządzeń klimatyzacyjnych, pomp wody chłodzącej i systemów wentylacyjnych. Powiązany sprzęt może ulec uszkodzeniu, chyba że zostanie szybko wyłączony lub przełączony na zasilacz awaryjny lub generator silnikowy. Niewiele zakłóceń zasilania natychmiast zniszczy obwody lub systemy awaryjne, ale większość z nich może spowodować skumulowane uszkodzenia. Każdy incydent może osłabić obwody elektroniczne, które ostatecznie ulegną awarii bez wyraźnego powodu. Często obwinia się słabą jakość sprzętu, ponieważ efekt kumulacji nie został rozpoznany, a sprzęt zastępczy prawdopodobnie wkrótce również zawodzi. Zakłócenia zasilania można zmierzyć, aby określić, czy dany obwód wydaje się być czysty. Zwykle urządzenie rejestrujące jest pozostawione na miejscu przez co najmniej tydzień, aby zmierzyć i zarejestrować szczegóły każdego zdarzenia, które ma miejsce. (Unikaj wszelkich przyrządów testowych, które rejestrują jedynie nienazwane zdarzenie, ale nie dostarczają żadnych szczegółów.) Niezależny inżynier, który nie jest sprzedawcą, może najlepiej przeprowadzić testy, które są obiektywne, kompleksowe i obejmują cały zakład. Niektóre obwody mogą wykazywać sporadyczne zakłócenia spowodowane przez coś w pobliżu

lub w budynku, a czasem przez wadliwe okablowanie. Wiedza o tym, jakie problemy z zasilaniem pojawiają się za pośrednictwem usługi głównej, pomaga określić, czy dostawca jest uszkodzony i określić, gdzie w budynku mogą powstać inne zakłócenia. Rzeczywiście, może być wiele przyczyn zakłóceń zasilania, a wszystkie z nich mogą być przerywane, dlatego zalecane jest ciągłe siedmiodniowe, 24-godzinne monitorowanie. Innym poważnym problemem elektrycznym jest nieprawidłowe uziemienie, które może uszkodzić wrażliwy sprzęt i powodować zakłócenia w kablach. Elektrycy muszą przestrzegać krajowych i lokalnych przepisów elektrycznych, ale niekoniecznie rozumieją lub zapewniają specjalne uziemienie niezbędne dla wrażliwych platform IS. Większość producentów sprzętu ciężkiego wymaga, aby każda jednostka miała izolowane połączenie uziemiające z dedykowanym przewodem drogi powrotnej do głównej magistrali uziemiającej budynku. Kilku producentów nie dostarcza specyfikacji instalacji, chyba że zostaniesz o to poproszony, a niektórzy instalatorzy ignorują je, aby zachować konkurencyjność cenową. Opinie są różne co do najlepszej konfiguracji podłoża pod budowę systemów informatycznych, a ponieważ warunki lokalne mogą się znacznie różnić, żadne podejście nie jest najlepsze. Warto skonsultować się z niezależnym inżynierem w celu sprawdzenia konfiguracji uziemienia oraz zalecenia i poświadczenia zgodności z lokalnymi przepisami. Ważne jest również zapewnienie oddzielnych obwodów dla wszystkich urządzeń IS, a tam, gdzie sprzęt jest podłączany do gniazda, nie ma więcej niż jednego gniazda. Oddzielne wyłączniki są zwykle wymagane dla wszystkich urządzeń, które mogą pobierać duży prąd, zwłaszcza jeśli obciążenie może się włączać i wyłączać. Jest to wymagane przez kod dla dużych silników, takich jak pompy, klimatyzacja i windy, których cykle mogą powodować zanieczyszczenie mocy w innych obwodach odgałęzionych. Ale kopiarki i duże drukarki laserowe (zwłaszcza starsze) mogą również powodować zakłócenia elektryczne podczas uruchamiania i podczas cyklu nagrzewnicy. Wszystkie rodzaje świateł mogą powodować zapad lub gwałtowny wzrost, gdy wiele urządzeń jest włączanych lub wyłączanych jednocześnie. (Nowsze światło fluorescencyjne oprawy ze statecznikami elektronicznymi oszczędzają energię i powodują znacznie mniej zakłóceń.) Oddzielne połączenie obwodu w pewnym stopniu izoluje przewody pod napięciem i neutralne od innych obwodów, ale zakłócenia mogą być generowane przez połączenia uziemiające, które często są połączone szeregowo z wieloma innymi obwodami, aby obniżyć koszty . Nie należy współużytkować wydzielonego obwodu z żadnym z tych urządzeń, które mogą łatwo zakłócać i uszkadzać sprzęt elektroniczny: znaczniki czasu, zszywacze elektryczne, dzbanki do kawy, lodówki, grzejniki, wentylatory lub jakiekolwiek inne urządzenie z silnikiem lub solenoidem. Nawet jeśli jest niedostępne, dedykowane gniazdko powinno być gniazdem pojedynczym, a nie dupleksowym. Dla odkurzaczy, elektronarzędzi lub sprzętu konserwacyjnego zbyt łatwo jest korzystać z drugiej połowy gniazda podwójnego. Spowoduje to poważne zakłócenia i może spowodować wyzwolenie wyłącznika. Musi istnieć wiele wygodnych gniazdek, które są łatwo dostępne dla wszystkich niekrytycznych potrzeb. Kolejną przyczyną problemów z zasilaniem jest nadmierna aktywność słoneczna. Zdarzenia te można zmierzyć tylko wtedy, gdy wystąpią, co jest przypadkowe w nieprzewidywalnym okresie kilku lat, którego szczyt przypada co około 11 lat. Zakłócenia słoneczne występują tylko w ciągu dnia. Wysoka aktywność słoneczna wystąpiła w 1988 roku, powodując poważne przerwy w dostawie prądu i zakłócenia radiowe w Montrealu w Kanadzie. Codzienne raporty o aktywności słonecznej, prognozy, zdjęcia i zapisy historyczne są dostępne pod adresem www.dxlc.com/solar i na innych stronach. W przypadku podejrzenia, napotkania lub nawet możliwości wystąpienia zakłóceń zasilania istnieje kilka możliwości zaradczych

1. Wyeliminuj problem w panelu dystrybucji zasilania. Pomocne mogą być lepsze uziemienie, więcej oddzielnych obwodów, tłumików, filtrów i transformatorów izolujących. Ale tego typu środki zaradcze mogą być trudne, kosztowne lub zawodne.

2. Użyj tłumika przepięć w pobliżu chronionego sprzętu. Jest to niedrogie, ale bezużyteczne w przypadku awarii zasilania, przerw w dostawach i poważnych zakłóceń.

3. Zastosuj zasilacz bezprzerwowy (UPS), który zapewnia zapasowe zasilanie bateryjne dla każdego elementu infrastruktury krytycznej. Jeden typ zasilacza UPS jest aktywowany tylko w przypadku awarii zasilania wejściowego, chociaż jego bateria jest zawsze ładowana. Lepszy typ jest zawsze w trybie online, działając w celu filtrowania przychodzącej mocy, tłumienia większości przepięć, kompensacji niewielkich przerw w dostawie i utrzymywania pełnej mocy systemu przez pięć do 10 minut po awarii - wystarczający czas, aby umożliwić prawidłowe zamknięcie systemu. Trzeci i najlepszy typ zasilacza UPS zawsze zasila swoje obciążenie z akumulatorów, izolując w ten sposób obciążenie od linii energetycznej i zapewniając optymalną ochronę.

4. W przypadku systemów, które pobierają dużą moc, zespół silnik-generator (MG) wyeliminuje większość problemów z zasilaniem. Zestaw MG to silnik elektryczny napędzany energią elektryczną. Silnik jest połączony z generatorem, który zawsze dostarcza czystą moc do obciążenia. Generator jest zwykle regulowany napięciem automatycznie, chociaż częstotliwość może się zmieniać, co może zakłócać niektóre obwody czasowe. Zwykle w przypadku przerwy w zasilaniu mechaniczny pęd jednostki zapewni wystarczającą moc do uporządkowanego wyłączenia sprzętu. Generatory silnikowe są nadal używane do ostatecznej filtracji i regulacji, ale musi istnieć elektryczne obejście, aby ułatwić konserwację.

Zasilacze UPS powinny zasilać i chronić serwery, sprzęt sieciowy i telefoniczny, komputery i krytyczne monitory. Większość zasilaczy UPS zapewnia gniazda bez rezerwowego zasilania, ale z tłumieniem szumów dla drukarek, „cegieł" transformatorów, faksów i urządzeń peryferyjnych, które nie muszą być stale włączone. Większość z tych urządzeń jest w pewnym stopniu zużywalna i szybko zastąpiona przez zespoły zapasowe, jeśli któreś jest uszkodzone. Poszczególne jednostki UPS, umieszczone w pobliżu chronionego sprzętu, kosztują mniej i mogą być wyłączone przez operatora, aby lepiej chronić sprzęt, który może być wrażliwy, nawet gdy sprzęt jest już wyłączony. Może to zapewnić dodatkową warstwę ochrony w przypadku uderzenia pioruna. Większe zasilacze UPS są używane w pomieszczeniach sprzętowych, gdzie mogą również monitorować i rejestrować wszystkie zdarzenia dotyczące zasilania oraz wyzwalać zdalne wskazania alarmowe. Większość dobrych zasilaczy UPS może zainicjować automatyczne wyłączenie sprzętu w przypadku awarii zasilania, rozładowania akumulatorów UPS lub ręcznej interwencji. Może jednak wystąpić problem, gdy niektóre z chronionych urządzeń nie mogą zostać ponownie uruchomione, dopóki baterie UPS nie zostaną w pełni naładowane. Niektóre zasilacze UPS są również urządzeniami sieciowymi, które mogą zgłaszać swój stan do zdalnej lokalizacji. Wiele zasilaczy UPS zapewnia również filtrowanie i tłumienie linii telefonicznych i Ethernet, a te funkcje powinny być używane, jeśli to możliwe. Piorun przenoszony przez przewody komunikacyjne może łatwo uszkodzić aparaty telefoniczne i modemy. Skoki napięcia i linii komunikacyjnej mogą występować asymetrycznie i mogą zniszczyć sprzęt, którego samo zakłócenie nie spowodowałoby. Dobry zasilacz UPS z tłumieniem linii komunikacyjnej jest w stanie najlepiej zatrzymać oba typy skoków. Inną zaletą zasilaczy UPS jest to, że gdy generator awaryjny jest włączony, energia elektryczna jest zwykle znacznie brudniejsza niż normalnie. Dodatkowa filtracja i stabilizacja zapewniana przez zasilacze UPS mogą stanowić różnicę między działaniem sprzętu IS a awarią

Zasilanie awaryjne

Większość krytycznych systemów i infrastruktury musi pozostać w pełni sprawna podczas jakiegokolwiek problemu z zasilaniem elektrycznym. Filtracja i tłumiki nie są w stanie zrekompensować przerw w zasilaniu, radzić sobie z większością zaników prądu ani z dużymi zakłóceniami elektrycznymi. Zakłócenia mogą pochodzić od wyładowań atmosferycznych (nawet jeśli jest zbyt daleko, aby je zobaczyć lub usłyszeć), silnej aktywności słonecznej lub zakłóceń o częstotliwości radiowej, które uszkadzają zasilanie sieciowe. Jednostki UPS mogą poradzić sobie z niektórymi z tych warunków, ale tylko krótko. Dlatego zapasowy generator awaryjny może być jedynym sposobem na kontynuowanie

pracy podczas długotrwałych problemów z zasilaniem. Chociaż generatory zapasowe są często jedyną alternatywą, nie są one panaceum. Generatory są drogie i skomplikowane w instalacji, wymagają co najmniej comiesięcznych ćwiczeń i nie zawsze są niezawodne. Ich regulacja napięcia jest marginalna; Podczas nagłych zmian obciążenia, napięcie wyjściowe i częstotliwość również mogą się zmieniać. Wraz ze wzrostem obciążenia pobierany jest większy prąd, a jeśli generator jest przeciążony, napięcie spada, a częstotliwość może spaść poniżej 60 Hz (co może zakłócić obwody czasowe IS). Ponieważ prąd obciążenia rośnie, aby sprostać zapotrzebowaniu na moc, ilość ciepła wytwarzanego przez zasilany sprzęt wzrośnie do kwadratu prądu. Większość urządzeń IS zasilanych jest indukcyjnie i po włączeniu lub ponownym uruchomieniu może wystąpić duży skok mocy rozruchowej. Dlatego generatory muszą mieć wystarczającą rezerwę mocy, wykraczającą poza przewidywane obciążenia sprzętu. Biorąc pod uwagę ich koszt, wytwórcy powinni mieć również wystarczające rezerwy mocy na przyszłość. Inną kwestią jest to, czy konkretny generator może zapewnić dostatecznie „czystą" energię elektryczną do obsługi sprzętu IS, jak również zasilania na inne potrzeby awaryjne obiektu. Dlatego należy upewnić się, że określony generator ma wystarczającą moc i jest przeznaczony do użytku ze sprzętem elektronicznym. Nawet wtedy zakłócenia powodowane przez duże silniki lub systemy oświetleniowe mogą wpływać na sprzęt elektroniczny. Ponieważ generatory zapasowe są drogie i złożone, planowanie jest często krótkowzroczne, a wiele instalacji nie jest dobrze zaprojektowanych lub odpowiednio przetestowanych. Nieuniknionym rezultatem jest to, że wiele generatorów nie działa zgodnie z oczekiwaniami. Oto kilka przykładów tego, co można przeoczyć. Po długiej dyskusji w dużym banku centralnym na Manhattanie na temat tego, co wydawało się być nadmiernym kosztem generatora zapasowego, projekt został niechętnie zatwierdzony. Generator miał zasilać dwa identyczne systemy komputerowe, tandem do wspierania krytycznej operacji handlu papierami wartościowymi. Ponieważ generator faktycznie kosztowałby więcej niż dwa komputery, koszt był problemem, dopóki bank nie zdał sobie sprawy, że generator zwróci się w ciągu jednego dnia użytkowania. Wkrótce po ukończeniu nastąpiła nagła awaria w całym mieście, która trwała trzy dni. Pomimo wielu niedogodności przy przenoszeniu paliwa z windy po schodach do generatora na dachu, jednostka działała bez zarzutu - był to jeden z nielicznych systemów na Manhattanie. Wiele innych generatorów nie uruchomiło się lub wyłączyło prawidłowo, pomimo ciepłej i dobrej pogody. A inni nie wspierali niezbędnej infrastruktury. W niektórych instalacjach nie uwzględniono wymagań dotyczących zasilania HVAC, więc komputery musiały zostać wyłączone w ciągu kilku minut, aby uniknąć przegrzania, mimo że była dla nich wystarczająca moc elektryczna. Zaniedbano moc generatora dla innych niezbędnych funkcji pomocniczych. Obejmowały one elementy sieci i systemy łączności, oświetlenie dla użytkowników, windę dostępną dla kluczowych osób i do transportu paliwa do generatora, systemy bezpieczeństwa i kontroli dostępu, a także przynajmniej podstawowe zaopatrzenie elektryczne w żywność i odpoczynek dla tych, którzy utrzymują podstawowe systemy w ruchu. . Bardzo niewiele firm uważało, że w swoich awaryjnych systemach zasilania uwzględniają wszystkie niezbędne funkcje wspomagające. Ten incydent wydarzył się kilka lat temu, kiedy przerwy w dostawie prądu uznano za bardzo mało prawdopodobne na Manhattanie. Generatory były wtedy swego rodzaju symbolem statusu. Ale dzisiaj nagłe awarie są znacznie częstsze. Podobny przykład krótkowzroczności miał miejsce w dużym podmiejskim luksusowym hotelu należącym do prestiżowej sieci hotelowej. Po gwałtownej burzy zakład energetyczny poinformował hotel, że musi stracić energię na kilka godzin, aby naprawić uszkodzoną podstację. Biorąc pod uwagę duże powiadomienie, hotel ustawił setki świec na korytarzach, w jadalni, salonie, recepcji i przy basenach, a następnie uruchomił generator awaryjny, który automatycznie wyłącza się, gdy tylko nastąpiła przerwa w dostawie prądu. Znaki ewakuacyjne i światła awaryjne na korytarzach i schodach działały prawidłowo. Zgodnie z oczekiwaniami baterie szybko się wyczerpały, ale świece działały długo i dobrze. Generator zasilał również jedną windę, system komputerowy i telefoniczny, system kontroli dostępu oraz wszystkie zamki w pokojach. Generator działał zgodnie z oczekiwaniami, ale proces reagowania awaryjnego nie. Nawet przy

wystarczającym ostrzeżeniu nikt nie pomyślał o zamknięciu innych wind lub umieszczeniu znaków nakazujących korzystanie ze schodów. Dwie bardzo przestraszone osoby zostały uwięzione w ciemności między piętrami, udowadniając, że generator może być obciążeniem, a nie korzyścią, chyba że procedury operacyjne są starannie zaplanowane, dobrze wdrożone i okresowo sprawdzane. Lista kontrolna bezpieczeństwa powinna być używana przy każdym uruchomieniu generatora. Inny niedawny przykład dotyczy stanowego centrum dowodzenia operacjami ratunkowymi, zaprojektowanego tak, aby pozostawało bezpieczne iw pełni funkcjonalne bez względu na to, jakie zdarzenia mogą wystąpić. Duży generator zasilał wszystkie krytyczne systemy. Wszystko było wielokrotnie testowane i działało zgodnie z oczekiwaniami. Ale potem pojawiły się kłopoty podczas ciężkich burz z piorunami w pobliżu. Energia elektryczna w większości miasta migotała kilka razy, a potem wracała do normy. Jednak generator próbował uruchomić się przy pierwszych oznakach kłopotów, a następnie zawahał się, gdy moc powróciła. Kilka sekund później, gdy zasilanie ponownie zamigotało, system generatora został uszkodzony i nie mógł się uruchomić. Stan miał szczęście, że generator nie był wtedy potrzebny, ale był nieobecny przez kilka dni do naprawy. Większość awarii zasilania zaczyna się od migotania i chwilowych przerw, które mogą unieruchomić system generatora, który nie jest prawidłowo skonfigurowany. Większość generatorów o znaczeniu krytycznym jest skonfigurowanych tak, aby uruchamiać silnik automatycznie, a wiele z nich automatycznie przekazuje moc, gdy tylko generator osiągnie prędkość. Ręczne uruchamianie i przenoszenie jest bardziej niezawodne i tańsze, jeśli zawsze dostępny jest przeszkolony personel. Najlepszy sposób na sekwencjonowanie następuje automatyczne działanie.

1. Po pierwszym sygnale rozruchu, sekwencja rozruchu musi trwać do uruchomienia silnika, przekroczenia limitu czasu nieudanego rozruchu lub ręcznego przerwania sekwencji.

2. Zasilanie nie jest przekazywane, dopóki generator nie osiągnie pełnej prędkości, w niezawodnej temperaturze roboczej, a zasilanie sieciowe nie nadaje się do użytku. Wszystkie trzy warunki powinny wystąpić przed przeniesieniem; mogą również wystąpić ręczne nadpisania.

3. Wszystkie przełączenia z powrotem do zasilania i wyłączenie generatora należy wykonać ręcznie. Najlepiej jest również móc indywidualnie przełączać każdy obwód do zasilania sieciowego.

Istnieje niezliczona ilość przykładów krytycznych generatorów kopii zapasowych, które nie działają zgodnie z oczekiwaniami. Oto kilka sugestii dotyczących określenia, czy generator jest niezbędny do ochrony systemów informatycznych oraz jak efektywnie i ekonomicznie wykorzystać generator.

* Zbadaj historię przerw w dostawach mediów, które obsługują lokal. Przedsiębiorstwo energetyczne zazwyczaj może dostarczyć te dane; jeśli nie, zwykle może to zrobić stanowa Komisja ds. Usług Publicznych. Pamiętaj, aby zapytać, jak zdefiniowano terminy, ponieważ „przestój” może obejmować tylko przerwy trwające dłużej niż kilka minut. Zapytaj również, czy są dostępne bardziej niezawodne podajniki. Podajniki pętli zasilane z obu końców są bardziej niezawodne i często obsługują krytyczny sprzęt. Zapytaj, czy transformatory rozdzielcze izolują i odfiltrowują zakłócenia zasilania, czy mogą również regulować napięcie wejściowe, a jeśli tak, specyfikacje.

* Dowiedz się, którzy inni klienci mają te same podajniki i odwiedź ich, aby omówić ich doświadczenia i określić, czy używają ciężkich maszyn. Chociaż niektóre zabezpieczenia są możliwe i mogą wiązać się z niewielkim lub żadnym kosztem dla klienta użyteczności publicznej, historia nie zawsze jest wiarygodnym przewodnikiem na przyszłość. Sieć dystrybucji zmienia się wraz z dodawaniem większych obciążeń. Obecnie zagrożenie przedłużonymi problemami z zasilaniem jest znacznie większe niż w przeszłości i szybko rośnie. Zasilacze UPS, zespoły silnikowo-prądnicowe i generatory zapasowe mogą być niezbędne w zastosowaniach o znaczeniu krytycznym.

* Określ, które z elementów infrastruktury IS wymagają zasilania awaryjnego z generatora awaryjnego. Większość krytycznych systemów informacyjnych, sprzętu, sieci i infrastruktury musi zawsze mieć najwyższą wydajność. I tak muszą być wszystkie obszary biurowe, systemy pomocnicze, media i personel potrzebny do ich obsługi. Przerwy mogą trwać dni lub tygodnie, a kluczowe osoby są odizolowane i mieszkają w obiekcie, aby systemy działały. Moc generatora musi spełniać wszystkie te potrzeby.

* Rozważ te systemy wsparcia, które mogą wymagać zasilania awaryjnego:

- Wszystkie systemy bezpieczeństwa SI, urządzenia zabezpieczające i monitorujące; systemy nadzoru obwodowego i kontroli dostępu, stacje ochrony i konsole.

- Schody przeciwpożarowe (które mogą stać się głównym środkiem wejścia i wyjścia), drzwi ewakuacyjne, alarmy przeciwpożarowe i domofony, których baterie szybko się rozładują. Również konieczność natychmiastowego rozpoczęcia ładowania tych akumulatorów, gdy tylko dostępne będzie zasilanie rezerwowe.

- Systemy ogrzewania, wentylacji, klimatyzacji (HVAC) i chłodzenia procesów, w tym wszystkie układy sterowania, wentylatory, pompy i zawory potrzebne do obsługi systemów krytycznych i wspomagających. Oprócz chłodzenia sprzętu, najlepiej zapewnić komfort w pomieszczeniu dla użytkowników, operatorów i administratorów. Klimatyzacja powierzchniowa może nie być możliwa, ale konieczne będzie przynajmniej dodatkowe ogrzewanie zimą i odpowiednia wentylacja.

- Wystarczające oświetlenie dla kluczowego personelu, pomieszczeń technicznych, szaf użytkowych, korytarzy, toalet i punktów gastronomicznych. Wiele pojedynczych włączników światła może oszczędzać energię i paliwo generatora. Światła na baterie nadają się tylko do natychmiastowego wyjścia awaryjnego i nie zapewniają oświetlenia obszaru.

- Wystarczająco dużo wygodnych gniazdek na sprzęt testowy, światła robocze i wszelkie akcesoria, które muszą być używane. W przypadku wentylatorów przenośnych mogą być również potrzebne gniazda pod napięciem.

- Wystarczający sprzęt gastronomiczny i urządzenia chłodnicze, bieżąca woda i urządzenia sanitarne, a także miejsce do spania dla operacji 24/7, które mogą trwać kilka dni.

- Winda zapewniająca krytyczny dostęp do miejsca, w nagłych przypadkach medycznych, dostarczanie żywności i zapasów oraz do transportu paliwa do generatora.

* Sporządź listę wszystkich elementów, które generator musi zasilać. Następnie zsumuj moc znamionową każdego elementu, aby określić rozmiar generatora i liczbę potrzebnych obwodów. Moce znamionowe sprzętu są zwykle pokazane na tabliczce znamionowej w pobliżu złącza zasilania i wymienione w instrukcjach. Oceny mogą być podawane w watach, amperach lub woltoamperach. Ogólnie przyjmuje się, że waty i woltoampery są równoważne. Ta ostatnia wartość jest wynikiem pomnożenia napięcia znamionowego (np. 120 woltów) przez znamionowe ampery, podczas gdy pierwsza mnoży tę liczbę przez współczynnik mocy sprzętu. Duże generatory mają moc znamionową w kilowatach (1000 watów). Jednostki przeznaczone do krótkich cykli pracy kosztują mniej i mogą ulec awarii podczas długotrwałej, ciągłej pracy. Doświadczony inżynier powinien przejrzeć ten proces.

* Weź pod uwagę koszty godzinowe utraty produktywności, działalności i wartości firmy w przypadku awarii jakichkolwiek systemów informatycznych. Dodaj do tego koszty odzyskiwania. W podanym wcześniej przykładzie banku pierwszy dzień, w którym generator był potrzebny, pozwolił zaoszczędzić

cały koszt systemu zasilania awaryjnego. Drugi i trzeci dzień tej szczególnej przerwy był dla banku czystą radością, ponieważ większość konkurentów zawahała się.

Przepisy elektryczne mogą wymagać, a dobra praktyka nakazuje, aby generator był tak dobrany, aby obsługiwał sumę poszczególnych obciążeń rozruchowych. Może się to wydawać marnotrawstwem, ponieważ nie wszystkie obciążenia uruchamiają się od razu, a średnie obciążenie robocze będzie nieco mniejsze niż suma części. Niemniej jednak rozsądną praktyką jest zapewnienie maksymalnego obciążenia znamionowego z dodatkową wolną pojemnością w celu zwiększenia niezawodności i przyszłych rozszerzeń. Istnieje kilka powodów przewymiarowania generatora. Gdy moc jest po raz pierwszy przekazywana do generatora, suma początkowych skoków może znacznie przekroczyć przewidywane obciążenie. Wszystkie jednostki UPS i inne urządzenia zasilane bateryjnie zaczną się ładować, a wszystkie silniki urządzeń mogą jednocześnie pobierać maksymalne prądy udarowe. Dodatkowa pojemność generatora zapewnia płynniejszy transfer z lepszą regulacją napięcia i zwiększa niezawodność systemu. Większość dużych generatorów wytwarza energię trójfazową. A każde z trzech wyjść powinno być zbalansowane, aby każda „noga" pobierała mniej więcej taką samą moc. Aby to zrobić, ciężkie silniki, wiele opraw oświetleniowych sterowanych jednym przełącznikiem i inne urządzenia wytwarzające przepięcia mogą wymagać podzielenia między trzy nogi. Istniejące okablowanie w panelach dystrybucyjnych prawdopodobnie będzie wymagało zmiany, aby zrównoważyć nogi. Pożądane jest, ale nie zawsze możliwe, zarezerwowanie jednej nogi na czystą moc dla krytycznych jednofazowych układów elektronicznych. Równoważenie każdej nogi to trudna sprawa, którą najlepiej wykonać w porozumieniu z niezależnym inżynierem. Jak najwięcej systemów elektronicznych, które są zasilane przez generator, powinno być również chronionych przez jednostki UPS, jak omówiono wcześniej, nawet jeśli dodają one do generatora , ładunek. Wystąpią duże skoki napięcia, zapady, zapady i stany przepięcia, gdy obciążenia generatora są przełączane i stale się zmieniają. Zakłócenia zasilania będą znacznie większe, ponieważ nie można odizolować elektrycznie hałaśliwych silników i oświetlenia. Zasilacze UPS powinny mieć również funkcję tłumienia szumów i regulację napięcia. A nawet przy tym wszystkim sprzęt IS będzie zestresowany i może zawieść. Zlokalizowanie generatora to kolejne wyzwanie. Do wyboru są na dachu lub w zabudowie, wewnątrz lokalu lub na zewnątrz. Każda witryna ma zalety i przeszkody. Generatory zewnętrzne mogą być najłatwiejsze i najtańsze w instalacji, ale także droższe w eksploatacji. Generatory zewnętrzne są hałaśliwe, często brzydkie, podlegają wandalizmowi, a lokalne rozporządzenia mogą je ograniczać. W przypadku umieszczenia na zewnątrz potrzebne są obudowy odporne na warunki atmosferyczne, aby chronić silnik, prądnicę i zbiornik paliwa. Większość silników używanych na zewnątrz wymaga ogrzewania, co może być dużym kosztem. Hałas to kolejny problem, a osoby znajdujące się w pobliżu mogą się sprzeciwiać. Ważne jest, aby używać dobrych tłumików i uzyskać pisemną zgodę od pobliskich właścicieli nieruchomości i innych najemców. Jednostki zewnętrzne powinny być ogrodzone z dużą ilością miejsca na konserwację i tankowanie. Jeśli to możliwe, najlepiej jest umieścić generator, ale nie zmniejsza to potrzeby ogrzewania i dobrego tłumika. Cała instalacja powinna być bezpiecznie zamknięta i chroniona alarmem otwarcia drzwi i czujnikami ruchu oraz znajdować się w zasięgu wzroku kamer monitorujących. Reflektory mogą odstraszać od wandalizmu i ułatwiać tankowanie. Generatory na dachach lub wady budynków stwarzają inne problemy, a te instalacje również mogą podlegać ograniczeniom wynikającym z lokalnych przepisów. Pierwszy problem to waga. Prawdopodobnie potrzebne będzie wzmocnienie konstrukcyjne. Następnym problemem jest umieszczenie jednostki na miejscu, co może wymagać dźwigu lub licencjonowanego riggera. Bardzo niewiele wind w budynku dociera na poziom dachu i mogą nie być w stanie obsłużyć nawet zdemontowanych części generatora. Może zaistnieć konieczność zamontowania wszystkich elementów generatora na zewnątrz budynku lub podniesienia ich po schodach pożarowych. Instalacje na szczycie cofnięć budynku będą wymagały specjalnych drzwi dostępowych, a przesuwanie ciężkiego sprzętu po gotowej podłodze wymaga

ciężkich desek i zabezpieczenia podłogi (np. Arkuszy masonitu lub sklejki) pod kółkami, aby uniknąć znacznego uszkodzenia podłogi. Na dachu lub cofce musi być wystarczająca ilość miejsca na paliwo i bezpieczną obsługę agregatu. Hałas będzie zwykle problemem, podobnie jak wibracje. Instalacje wewnętrzne oferują zarówno zalety, jak i wyzwania. Czasami wykonalne jest pomieszczenie wewnętrzne, ogrzewane pomieszczenie na parterze typu garażowego ze standardowymi drzwiami garażowymi otwieranymi podczas pracy generatora. Taki układ jest dobry, ponieważ jest niepozorny, ognioodporny, łatwy do ochrony i wygodny do tankowania i konserwacji. A w przypadku awarii generatora można łatwo podłączyć jednostkę zamontowaną na przyczepie. Wewnątrz generatorów mogą obowiązywać przepisy budowlane lub przeciwpożarowe. Potrzebne są duże pomieszczenia, aby ułatwić tankowanie i konserwację oraz duże systemy wentylacyjne, aby rozproszyć znaczne ciepło silnika. Wydech silnika może być dobrze stłumiony i wyprowadzony rurami na zewnątrz, podczas gdy powietrze wlotowe do silnika jest doprowadzane z zewnątrz. Ogrzewanie i wentylacja pomieszczenia muszą być odpowiednio zaprojektowane zarówno do bardzo gorącej, jak i bardzo zimnej pogody. Pomieszczenie musi być ognioodporne i dźwiękoszczelne, wyposażone w alarmy przeciwpożarowe i system gaszenia wykorzystujący chemikalia lub tryskacze z suchą głowicą, które nie mogą zamarznąć. Podłoga może wymagać wzmocnienia i wibroizolatorów. Odpływ podłogowy jest wskazany i musi być zatwierdzony pod kątem ochrony środowiska. Instalacje wewnętrzne mają zalety. Generator i jego paliwo można łatwo utrzymać w cieple. Uruchamianie jest łatwiejsze i bardziej niezawodne. Tankowanie jest łatwiejsze bez konieczności stawiania czoła żywiołom. Jest mniejsze prawdopodobieństwo, że paliwo dostanie się wody, co może być śmiertelne dla silników Diesla, a konserwacja jest znacznie łatwiejsza. Problemy z instalacjami budowlanymi obejmują przepisy budowlane, które dopuszczają tylko małe dzienne zbiorniki paliwa. Co kilka godzin należy wnosić dużo paliwa, aby generator mógł pracować. Paliwa nie można przechowywać w większości budynków, a winda może nie działać lub być dostępna, aby pomóc w wniesieniu kanistrów z paliwem. Istnieje wiele możliwych paliw do generatorów awaryjnych. Olej napędowy jest najbardziej wydajny, a silniki wysokoprężne mogą pracować nieprzerwanie przez wiele dni, ale trudno je uruchomić, zwłaszcza w niskich temperaturach, i nie można ich ręcznie obracać. Domowy olej opałowy jest w zasadzie taki sam jak olej napędowy i można go zastąpić w dowolnym momencie, gdy olej napędowy nie jest dostępny, ale wymaga to dodatkowego filtrowania paliwa. Jeśli używane jest paliwo płynne, zbiornik paliwa powinien być zawsze pełny, aby uniknąć kondensacji. Dodatki do paliwa mogą zapobiegać gumowaniu i wspomagać rozruch. Upewnij się, że cały olej napędowy jest przygotowany do użytku w zimnym klimacie. Rafinerie zwykle nie stosują tego procesu poza zimą, ale nieuzdatniony olej napędowy zamienia się w żel w pobliżu temperatur ujemnych i paliwo nie będzie płynąć. Nigdy nie pozwól dealerowi „przecinać" oleju napędowego naftą, która jest korozyjna. Olej napędowy wymaga również dodatków, aby uniknąć gromadzenia się bakterii, które zatykają przewody paliwowe. Powinny istnieć materiały czyszczące zatwierdzone przez OSHA, gotowe na wszelkie przyszłe wycieki lub wycieki. Gaz ziemny lub propan to najwygodniejsze paliwa. Każda z nich eliminuje zbiornik dzienny i tankowanie.

Silniki te są najmniej zanieczyszczające, uruchamiają się znacznie łatwiej, nie wymagają podgrzewania i można je ręcznie obracać. Jednak większość z nich nie jest przeznaczona do długotrwałej pracy ciągłej. Silniki benzynowe są zabronione przez wiele przepisów budowlanych i są rzadko używane, z wyjątkiem małych, przenośnych generatorów. Benzyna jest znacznie bardziej niebezpieczna w obsłudze i przechowywaniu, a silniki benzynowe nie wytrzymują zbyt dużego obciążenia. Stale monitoruj poziom oleju silnikowego i przygotuj się na dolewanie oleju, gdy tylko będzie to potrzebne. Większość generatorów wyłącza się automatycznie, gdy poziom oleju jest niski. Niektóre wyłączają się również po przegrzaniu. Każde nieoczekiwane wyłączenie generatora będzie katastrofalne, dlatego należy uważnie obserwować pod kątem wczesnych sygnałów ostrzegawczych o problemach. Po ustaleniu żądanego rozmiaru i typu generatora należy wziąć pod uwagę inne kwestie:

* Automatyczne sterowanie silnikiem i przełączniki przenoszenia obciążenia mogą być zawodne i mogą spowodować uszkodzenia. Unikaj ich, jeśli to możliwe. Jednak generatory mogą być monitorowane i sterowane zdalnie, a także na miejscu.

* Automatyczne uruchamianie może być zawodne. Jeśli silnik nie uruchomi się szybko, akumulator szybko się rozładuje, zwłaszcza silniki wysokoprężne w zimne dni, które wymagają grzejników świecowych. Jeśli to w ogóle możliwe, ktoś powinien być obecny podczas procesu uruchamiania, korzystając z listy kontrolnej w celu weryfikacji prawidłowego działania, a następnie ręcznie przenosząc obciążenie, gdy generator jest gotowy. Przełączniki, które automatycznie przenoszą obciążenie, są drogie i czasami zawodzą. Zawsze ręcznie przełączaj z powrotem do źródła zasilania i rób to dopiero po przełączeniu wrażliwych systemów w tryb czuwania. Automatyczny transfer może spowodować poważne szkody, jeśli napięcie sieciowe będzie migotać i ponownie znika lub jeśli napięcie lub częstotliwość wahają się podczas przesyłania, jak to często się dzieje. Nie wyłączaj silnika automatycznie. Najlepiej jest to zrobić ręcznie i nie przed płynnym zasilaniem sieciowym.

* Najlepsze przełączniki transferowe pozwalają na indywidualne przesyłanie każdego z głównych obwodów, aby zminimalizować nieuniknione fluktuacje, które mogą wystąpić, gdy wszystko jest przełączane jednocześnie.

* Generator awaryjny musi być regularnie uruchamiany. Producent określi, kiedy i jak należy ćwiczyć jednostki. Zwykle należy to robić co miesiąc i przy średnim lub dużym obciążeniu. W przypadku systemów krytycznych dobrą praktyką w zakresie bezpieczeństwa jest cotygodniowe uruchamianie generatora. Powinien istnieć pisemny, parafowany wpis do dziennika dla każdego zdarzenia, w tym każdego ćwiczenia, przeglądu, konserwacji, sprawdzenia oleju i tankowania. Zawsze rejestruj godziny pracy.

Pomimo kosztów i złożoności, istnieje duże zadowolenie z posiadania dobrego generatora awaryjnego, który działa płynnie, zwłaszcza gdy inne organizacje mogą się rozpadać. Gdy generator będzie działał dobrze podczas prawdziwego zagrożenia, nawet sceptycy zdają sobie sprawę z wartości dodanej.

Kontrola środowiska

Mimo że dzisiejsze systemy informacyjne nie wymagają tak dużo chłodzenia ani precyzyjnej kontroli środowiska, jakiej wymagały dawne systemy, dobra kontrola temperatury i wilgotności, dobra wentylacja i czyste powietrze są nadal ważne. Systemy informacyjne mogą działać niezawodnie tylko wtedy, gdy utrzymywane są odpowiednie środowiska zarówno w pomieszczeniach sprzętowych, jak i w miejscach pracy użytkowników. Ale każdy obszar wymaga innego podejścia. Klimatyzacja jest zasadniczo przeznaczona do chłodzenia ludzi; sprzęt powinien być chłodzony przez inny funkcjonalnie system, który najlepiej określa się mianem chłodzenia procesowego. Systemy nie powinny być mieszane, ani też jeden z nich nie powinien zastępować drugiego. Przepisy budowlane wymagają HVAC we wszystkich zajętych przestrzeniach, w których mogą gromadzić się ludzie lub gdzie znajdują się stacje robocze. Przepisy budowlane określają również minimalne wymagania dotyczące wentylacji dla zajmowanej przestrzeni, w tym minimalny procent powietrza uzupełniającego (zewnętrznego), który ma być stale doprowadzany do każdej zajmowanej przestrzeni, aby powietrze wewnątrz nie stało się zwietrzałe. Większość kodów nie uwzględnia potrzeb sprzętu elektronicznego. Sprzęt elektroniczny ma wiele specjalnych potrzeb, a wiele z nich jest niezgodnych z wygodami ludzi wymaganymi przez kodeksy. Większość urządzeń elektronicznych działa w sposób ciągły, podczas gdy klimatyzacja działa głównie w godzinach pracy. Systemy chłodzenia klimatyzacji mogą zostać wyłączone w celu konserwacji, podczas przerwy w dostawie prądu, po godzinach pracy lub w chłodne dni. Z kolei chłodzenie procesu musi działać w sposób ciągły i codziennie, dlatego często stosuje się systemy równoległe i nadmiarowe. To samo powietrze powinno być dobrze filtrowane i recyrkulowane bez

dodawania powietrza uzupełniającego w celu wprowadzenia kurzu lub zanieczyszczeń. Zmniejsza to również wymaganą wydajność chłodzenia, więc sprzęt do chłodzenia procesu może mieć mniejszą wydajność i być tańszy w eksploatacji. Sprzęt elektryczny i okablowanie również wymagają dobrej kontroli wilgotności, do której zapewnienia zaprojektowano systemy chłodzenia procesowego. Te systemy są zaprojektowane tak, aby były łatwiejsze i szybsze w czyszczeniu i konserwacji. Często wiele komponentów jest nadmiarowych i można je wymieniać podczas pracy.

Coraz częściej klimatyzator znajduje się na podłodze lub suficie pomieszczenia technicznego, przez co potrzeba mniej kanałów, przepustnic czy rejestrów. Cały sprzęt przetwarzający, magazynujący i sieciowy IS powinien znajdować się wewnątrz wydzielonych pomieszczeń sprzętowych, które również powinny być wyznaczone jako wolne przestrzenie, aby uniknąć narzuconych kodem wymagań dotyczących klimatyzacji. Unikaj używania terminów takich jak „sala komputerowa" lub „centrum danych", które są zwykle rozumiane jako miejsca zajęte. Zarówno chłodzenie procesu w pomieszczeniach sprzętowych, jak i klimatyzacja w miejscach pracy muszą zapewniać kontrolę wilgotności. Ważne jest, aby przez cały czas utrzymywać wilgotność względną w zakresie od 40 do 60 procent, niezależnie od klimatu i pory roku. Kiedy wilgotność względna spada poniżej 40 procent, co może się łatwo zdarzyć w zimne dni, podczas poruszania się ludzi generowana jest elektryczność statyczna. Ładunki statyczne mogą szybko się nagromadzić i osiągnąć wiele tysięcy woltów, a iskra przeskoczy na każdy obiekt, którego dotknie osoba, a który ma inny ładunek. Nawet jeśli takiej iskry nie da się wyczuć, kilka tysięcy woltów może zniszczyć obwody elektroniczne. Na przykład ładunek elektrostatyczny przeskakujący z opuszka palca na klawiaturę może spowodować poważne uszkodzenie nośników pamięci i obwodów. Wiele szkód może nie być od razu widocznych. Rzeczywista awaria może być opóźniona, więc przyczyna nie jest identyfikowana. Uziemione paski można instalować na stacjach roboczych, a personel serwisowy powinien nosić uziemione opaski na nadgarstek, chociaż nie eliminują one całkowicie problemu. Jedynym skutecznym rozwiązaniem jest zawsze utrzymanie względnej wilgotności powyżej 40 procent. Wilgotność względna powyżej 0 procent również powoduje problemy, które ostatecznie niszczą sprzęt i okablowanie. Powyżej 60 procent kondensacja i pleśń zaczną uszkadzać niektóre elementy. Powyżej około 80 procent zachodzi działanie galwaniczne, które ostatecznie spowoduje poważne problemy. Proces ten jest często nazywany migracją srebra, ponieważ większość połączeń elektronicznych jest posrebrzana. Zjawisko to jest podobne do elektrolizy (galwanizacji), ale tutaj dwa metale są zanurzone w wysokiej wilgotności, a nie w cieczy i nie ma zewnętrznego prądu potrzebnego do działania galwanicznego. Cząsteczki jednego przewodnika zaczynają fizycznie zbliżać się do drugiego i przyczepiać się do niego, mniej aktywnego metalu. Chociaż obie powierzchnie mogą być pokryte złotem, srebrem lub miedzią, prawdopodobnie różnią się nieznacznie składem. Dlatego działanie galwaniczne nastąpi, gdy wilgotność będzie zbyt wysoka. Styki i gniazda złączy mogą się rozpaść, stopić się lub uszkodzić elektrycznie z powodu wżerów. Obwody drukowane również mogą zawieść. Chociaż to galwaniczne działanie zachodzi powoli, kumuluje się i jest nieodwracalne. Awarie są zwykle bez ostrzeżenia i prawie zawsze winą jest raczej niska jakość niż wysoka wilgotność. Jedynym zabezpieczeniem jest kontrola wilgotności zarówno w pomieszczeniach sprzętowych, jak i obszarach roboczych. Systemy chłodzenia procesowego i klimatyzacji zwykle robią to na kilka sposobów. Oba systemy osuszają w sposób naturalny podczas chłodzenia i mogą wykorzystywać wężownicę do podgrzewania powietrza wylotowego, jeśli wilgotność jest zbyt niska. Również gdy wilgotność jest zbyt niska, woda jest dodawana za pomocą rozpylacza, atomizera lub mokrego sita, przez które przepompowywane jest powietrze nawiewane. Istnieją dodatkowe zabezpieczenia, które są rozsądne w instalacji i utrzymaniu. W zimnym klimacie wszystkie obszary i miejsca pracy wyposażone w sprzęt elektroniczny powinny mieć podłogi o niskim poziomie statyczności. Może to być wykładzina lub płytka podłogowa o niskiej statyczności, wykonana w tym celu. Nie polegaj na sprayach do kontrolowania elektryczności

statycznej; szybko się rozpraszają. Upewnij się, że ściany i drzwi pomieszczenia z wyposażeniem są dobrze uszczelnione, aby wilgoć, kurz i zanieczyszczenia nie mogły migrować. Upewnij się, że ściany są dobrze uszczelnione od płyty do płyty, a same płyty są nieprzepuszczalne dla kurzu i wilgoci.

Ochrona przed dymem i ogniem

W każdym pomieszczeniu sprzętowym należy zapobiegać powstawaniu dymu i ognia, ponieważ w przeciwnym razie szybko nastąpią znaczne uszkodzenia i zakłócenia. Bez względu na wielkość incydentu skutki dymu lub ciepła kumulują się. Systemy ostatecznie ulegną awarii i zwykle bez ostrzeżenia. Oczywiście, palenie tytoniu i innych substancji musi być zabronione, ale pokoje z wyposażeniem mogą być kuszące dla nieprzeszkolonego personelu, ponieważ te pokoje mogą wydawać się bezpiecznym, chłodnym miejscem do rzucania dymu - a nawet mogą być w dużej mierze bez opieki. Drzwi do pomieszczenia wyposażenia nie powinny być nigdy podparte przez personel sprzątający, dostawczy lub konserwacyjny lub inne osoby pracujące na zewnątrz, gdy klimatyzacja jest wyłączona. Pierwszym poziomem zapobiegania jest trzymanie wszystkiego, co palne, poza pomieszczeniami technicznymi. Papier i materiały eksploatacyjne, które nie są aktualnie używane, należy przechowywać na zewnątrz, nigdy w pomieszczeniu z wyposażeniem. Chociaż większość dokumentacji jest obecnie udostępniana elektronicznie, materiały referencyjne lub dokumenty dotyczące reagowania w sytuacjach awaryjnych, gdy systemy są wyłączone, mogą być przechowywane w pomieszczeniu; powinny one być przechowywane w ognioodpornych plikach lub szafkach bezpiecznych i szybki dostęp w nagłych wypadkach. W pomieszczeniu ze sprzętem nie powinno być żadnych pojemników na śmieci, a niszczarki powinny znajdować się na zewnątrz, pod ścisłą kontrolą. Powinna istnieć jasna i stanowcza polityka, zgodnie z którą nic łatwopalnego nie może pozostać w pomieszczeniu wyposażenia i należy przeprowadzać częste inspekcje w celu sprawdzenia zgodności. Pomieszczenia magazynowe sprzętu i dostawców powinny być zaprojektowane tak, aby chronić, a nie pomieścić ludzi. W pomieszczeniach wyposażenia nie powinno być żadnych zbędnych mebli, zwłaszcza biurek, które mogą być zagracone i które nie są klasyfikowane jako ognioodporne. Zwykle wystarcza metalowy stół z jedną małą szufladą i jednym lub dwoma metalowymi krzesłami z ognioodporną tapicerką. Nieodpowiednie zabezpieczenia przeciwpożarowe są głównym zagrożeniem, które często jest pomijane. Środek przeciwpożarowy to zwykle rękaw i specjalny materiał zapobiegający przedostawaniu się dymu lub ciepła do otworu w przegrodzie, podłodze lub suficie. Zatrzymuje również rozprzestrzenianie się płomienia. W całym obiekcie potrzebnych jest wiele ogniochronnych, w tym w rdzeniu budynku oraz obszarach mechanicznych, użytkowych i wyposażenia - nawet w parterowym budynku. Ogniochrony są rygorystycznie wymagane przez większość norm, ale zgodność jest często niewystarczająca, a urządzenia często są naruszane przez kolejne modyfikacje lub zmiany okablowania. Ściany działowe, ściany budynków, podłogi i sufity muszą mieć odporność ogniową zgodnie z krajowymi i lokalnymi przepisami budowlanymi oraz innymi przepisami. Właściwa konstrukcja jest zwykle określana przez architekta lub inżyniera, a zgodność jest sprawdzana lub certyfikowana zaraz po zakończeniu budowy. Inspekcja często ma miejsce przed ukończeniem wszystkich układów mechanicznych i instalacji okablowania. Następnie, jeśli jakiekolwiek przejście lub otwór zostanie wykonany przez ścianę, podłogę lub sufit, jego klasa przeciwpożarowa zostanie unieważniona i powinna zostać ponownie certyfikowana. Ściany wszystkich pomieszczeń technicznych muszą być konstrukcją typu płyta do płyty, bez dostępu do przepływu powietrza pod lub nad ścianami. Uznany autorytet ocenia i zatwierdza komercyjne zabezpieczenia przeciwpożarowe, zanim będą mogły być legalnie sprzedawane. Każdy producent określa następnie zatwierdzone zastosowania, procedury instalacji i konserwacji niezbędne do zapewnienia zgodności. Dlatego rozsądnie jest zatrudniać wyspecjalizowanych dostawców z rozległym przeszkoleniem i doświadczeniem w instalowaniu i sprawdzaniu zabezpieczeń przeciwpożarowych oraz zlecać im okresowe kontrole pomieszczeń i certyfikaty. Nieodpowiednie zabezpieczenia przeciwpożarowe są szczególnie częste w głównych

obszarach starszych budynków lub tam, gdzie najemcy zajmują kilka pięter. Chociaż podczas budowy mogły zostać zapewnione odpowiednie zabezpieczenia przeciwpożarowe, instalacja rur, kabli, przewodów i późniejsze zmiany okablowania często je naruszają. Przewody często przechodzą przez duże, ziejące otwory ukryte pod podwieszanym (podwieszanym) sufitem lub za stojakami na sprzęt lub korytami na przewody. Za każdym razem, gdy zajdą zmiany, należy zainstalować i sprawdzić odpowiednie zabezpieczenia przeciwpożarowe. Wielu instalatorów tego nie rozumie lub idzie na skróty, mając nadzieję, że nikt nie zauważy lub nie założy, że inni się tym zajmą. Bez odpowiednich zabezpieczeń przeciwpożarowych ogień i dym mogą i prawdopodobnie będą się rozprzestrzeniać zaskakująco szybko. I tak będzie proch. W przypadku odniesienia obrażeń przez ludzi lub uszkodzenia sprzętu z powodu niewłaściwych zabezpieczeń przeciwpożarowych lub nieodpowiedniej konstrukcji przeciwpożarowej mogą wystąpić poważne zobowiązania. Koszty, stracony czas i utrata reputacji będą ogromne. Okresowe i dokładne inspekcje przeciwpożarowe przeprowadzane przez niezależnego i wykwalifikowanego eksperta szybko wykryją naruszenia budynku i zabezpieczeń przeciwpożarowych. Dym jest znacznie bardziej niebezpieczny niż płomień. A cały dym jest toksyczny! Zawiera duże ilości tlenku węgla, który jest niewidoczny, bezwonny i szybko śmiertelny. Dym jest produktem spalania wielu materiałów, a oddychanie większości z nich jest niebezpieczne. Niektóre są śmiertelne. Nawet niewielka ilość dymu może spowodować poważne szkody dla ludzi i wiele szkód dla sprzętu elektronicznego. Dym jest zwodniczy; nawet jeśli wydaje się, że nie ma dużo dymu lub ciepła, a widoczność jest dobra, ludzie w obrębie obszaru lub przejeżdżający przez ten obszar szybko stają się niepełnosprawni, a niektórzy mogą wkrótce umrzeć. Pierwszym priorytetem jest bezpieczeństwo ludzi. Odciągnij wszystkich natychmiast od dymu, i trzymaj wszystkich z daleka. Tylko przeszkoleni ratownicy z odpowiednią odzieżą ochronną, sprzętem i niezależnym aparatem oddechowym powinni wchodzić do zadymionych obszarów. Ogólnie rzecz biorąc, maski oddechowe nie stanowią wystarczającej ochrony i mogą również przeciekać. Nie może być heroizmu; czołganie się przez dym na podłodze lub oddychanie przez mokrą szmatę to desperackie środki, które należy podejmować tylko wtedy, gdy nie można ich uniknąć, aby uciec z tego obszaru. Każdy powinien zaczekać w bezpiecznym miejscu na przybycie strażaków, a następnie postępować zgodnie z ich instrukcjami. Najlepszym sposobem uniknięcia pożaru w pomieszczeniu jest trzymanie wszystkiego, co palne, na zewnątrz pomieszczenia. Dokumenty, instrukcje i materiały należy przechowywać poza pokojem w zamkniętych metalowych szafkach. Meble wewnętrzne powinny być ograniczone do metalowego stołu i krzesła lub dwóch. Wszystkie pojemniki na odpady powinny znajdować się na zewnątrz. Po wyeliminowaniu materiałów palnych jedyny dym, który się pojawi, będzie pochodził z przegrzania elektrycznego. Pożary elektryczne rzadko występują w pomieszczeniu ze sprzętem, a te, które mają miejsce, są prawdopodobnie bardzo małe, krótkie i ustają, gdy tylko zostanie odłączona energia elektryczna. (Należy pamiętać, że większość komponentów komputerowych działa teraz przy napięciu 5 V lub mniej, więc zwarcie nie jest bardziej niebezpieczne niż na przykład zwarta latarka, która nie stanowi zagrożenia dymem.) Chociaż czasami zauważalnie gryzący, zwykle widoczny jest niewielki dym. . Dlatego czułe czujniki ognia i dymu oraz skuteczne środki gaszenia ognia są potrzebne i wymagane przez większość przepisów budowlanych i przeciwpożarowych. Dobre detektory mogą zapewnić wystarczająco wczesne ostrzeżenie, aby zapobiec problemom i obrażeniom. Wystarczająca ilość dymu lub ciepła, aby spowodować rzeczywiste uszkodzenie sprzętu, wymaga prądu elektrycznego wyższego niż większość komponentów może pobrać. Wyłączniki automatyczne i bezpieczniki zwykle otwierają się, zanim pojawi się dużo dymu lub nastąpi uszkodzenie. Być może największym zagrożeniem jest dym ze stateczników w niskiej jakości oprawach fluorescencyjnych, który może wydzielać znaczne ilości czarnego dymu. Dym jest żrący i może skraplać się na złączach i obwodach drukowanych, co może w końcu ulec awarii. W każdym pomieszczeniu sprzętowym powinny znajdować się czujniki dymu, które są podłączone do centralnego systemu alarmowego. Powinno być wystarczająco dużo detektorów, aby pokryć całą objętość każdego pomieszczenia. Każdy detektor powinien zawierać elektryczne oko do wyszukiwania zamglenia lub

dymu, czujniki jonizacyjne do wykrywania produktów spalania na długo, zanim jakiekolwiek zostaną zauważone przez ludzi, oraz czujniki szybkiego wzrostu temperatury, na wypadek gdyby nagromadziło się wystarczająco dużo ciepła, aby spowodować uszkodzenie. Pomimo wykrycia nic nie powstrzyma dymu wytwarzanego przez przegrzane przewody lub komponenty, dopóki nie zostanie odcięte zasilanie elektryczne lub inne źródło ciepła nie zostanie usunięte. W każdym pomieszczeniu technicznym musi znajdować się system tłumienia ognia. Wymaga tego zarówno zgodność kodu, jak i dobra praktyka bezpieczeństwa. Tłumienie pożaru najlepiej jest osiągnąć za pomocą głowic zraszaczy, które rozpylają mgłę wodną, nawet jeśli niektóre niezabezpieczone urządzenia mogą zostać uszkodzone, jeśli woda nie będzie szybko działać. W pobliżu sprzętu często znajdują się specjalne wodoodporne osłony ochronne na wypadek wypadków, takich jak wycieki z sufitu lub uszkodzenie głowicy tryskacza. Ale jeśli obszar jest już zadymiony, nikt nie powinien próbować zakładać osłon. Okablowanie, połączenia i większość komponentów wysychają, nawet po zamoczeniu. Proces można przyspieszyć ręcznikami niepozostawiającymi włókien i ostrożnym użytkowaniem suszarek do włosów. Klawiatury, monitory, zasilacze UPS, zasilacze, niektóre napędy dyskowe lub taśmowe, a zwłaszcza drukarki, mogą ulec uszkodzeniu i należy je wymieniać do czasu ich sprawdzenia. Dyski twarde są zwykle hermetycznie zamknięte i nienaruszone. Kilka innych elementów może zostać uszkodzonych przez nadmierne ciepło, chociaż mgła wodna jest bardzo skuteczna w hartowaniu źródeł ciepła. W pobliżu powinno być bezpiecznie przechowywanych wiele elementów zastępczych. Manipulowanie uszkodzonymi komponentami niskonapięciowymi (takimi jak większość płytek drukowanych) nie stanowi większego zagrożenia dla ludzi - pod warunkiem, że nie ma za dużo wody, a osoba wie, co robią i jak uniknąć uszkodzenia komponentów. W razie wątpliwości tymczasowo wyłącz komponenty. Zamknięte szafy sprzętowe zapewniają najlepszą ochronę niezależnie od systemu tłumienia ognia w pomieszczeniu. Zamknięte szafki mogą monitorować temperaturę i wilgotność, wykrywać i powstrzymywać dym, alarmy dźwiękowe i często zawierają systemy tłumiące pożar, zanim wystąpią problemy. Środek gaśniczy Halon 1301 był kiedyś szeroko stosowany w krytycznych obszarach. Ale halon to fluorowęglowodór, którego produkcja jest zakazana od wielu lat. Dzisiejsze systemy chemiczne są projektowane inaczej; jeden przykład wykorzystuje środek tłumiący FM200 firmy Siemens. Rzekoma zaletą chemicznych środków tłumiących jest to, że ludzie mogą oddychać środkiem, przynajmniej podczas opuszczania obszaru. Inny system gaszenia pożarów wykorzystuje dwutlenek węgla, który jest skuteczny i tańszy, ale może ugasić ludzi, a także pożary. Problem ze wszystkimi środkami chemicznymi, w tym dwutlenkiem węgla, polega na tym, że szybko mieszają się z dymem i stają się bardzo toksyczne. Sam środek może być bezpieczny do oddychania, ale zmieszany z nim dym nie. Te systemy są również bardzo drogie. Niezależnie od systemu gaszenia, w pobliżu wyjścia z pomieszczenia powinny znajdować się elementy sterujące i odcinające, ale niedostępne dla sprawcy. Ogólnie rzecz biorąc, słyszalny, ciągły alarm wskazuje, że zaraz zostanie uruchomiony system tłumienia. Na panelu sterowania powinny znajdować się przyciski odroczenia, a być może również zdalne, które opóźnią aktywację o około dwie minuty, podczas gdy ktoś interweniuje. W trybie odroczenia generowany jest sygnał dźwiękowy. Cichy alarm powinien pozostać aktywowany, gdy system gaszenia pożaru zostanie wyłączony lub alarmy zostaną wyciszone. Następny poziom ochrony wykorzystuje kilka gaśnic. Są to najbardziej przydatne zabezpieczenia, ponieważ tłumik można skierować tam, gdzie jest potrzebny, a nie na całe pomieszczenie. Dwutlenek węgla jest najlepszy, ponieważ nie pozostawia osadu. Gaśnice chemiczne, proszkowe i piankowe również działają dobrze, ale trudno je wyczyścić. Gaśnice typu ABC są najlepsze, ponieważ są skuteczne odpowiednio w przypadku materiałów łatwopalnych, łatwopalnych cieczy i pożarów elektrycznych. Kilka ręcznych gaśnic jest lepszych niż kilka dużych, ciężkich jednostek. Wszystkie gaśnice powinny być w widoczny sposób zamontowane na ścianie lub umieszczone bezpośrednio wewnątrz i na zewnątrz wejść. Zatwierdzona przez OSHA czerwona naszywka umieszczona na ścianie najbliżej każdej gaśnicy podkreśla jej lokalizację. Zapoznaj się również z innymi wymogami BHP, kodeksem lokalnym i wymaganiami dotyczącymi ubezpieczenia,

które mogą mieć zastosowanie. Powietrze nawiewane z urządzeń do chłodzenia procesu powinno być szybko i automatycznie wyłączane, aby uniknąć recyrkulacji dymu. Niedługo potem może być konieczne wyłączenie sprzętu IS, zanim się przegrzeje. Najlepiej jest wyłączyć wszystko szybko i automatycznie w uporządkowanej sekwencji - chłodzenie, sprzęt IS, zasilanie elektryczne i oświetlenie - a następnie ewakuować. Wyłącz oświetlenie, na wypadek gdyby było to częścią problemu. Wyłączenie powinno nastąpić automatycznie z ręczną interwencją ze sterowania w pomieszczeniu lub zdalnie. Zalecane jest zasilane bateryjnie oświetlenie wyjścia i pomieszczenia awaryjnego, aby ratownicy nie potrzebowali latarek. Tak zwany wózek awaryjny to dobra inwestycja. Jest to używane podczas stanu dymu, wycieku wody i, miejmy nadzieję, przed aktywacją systemu przeciwpożarowego. Wózek zderzeniowy jest trzymany na zewnątrz lub w pobliżu głównych pomieszczeń sprzętowych i przetaczany tam, gdzie jest potrzebny. Wózek zwykle zawiera osłony zapobiegające przedostawaniu się dymu i wody do stojaków i sprzętu, duże gaśnice, a czasem respiratory lub niezależne aparaty oddechowe. Wózek awaryjny powinien zawierać procedury szybkiego odniesienia oraz listę kontrolną dotyczącą ochrony i zamykania pomieszczenia, a także procedury bezpieczeństwa i powiadamiania - zwykle drukowane na plastiku. Wózek zderzeniowy należy sprawdzać co miesiąc, a procedury przeglądać, a także organizować okresowe szkolenia i ćwiczenia w celu ćwiczenia obsługi sprzętu. Przed użyciem osłon przeciwdymowych i wodnych należy najpierw wyłączyć zasilanie urządzenia. Wózki awaryjne były ważne we wczorajszych salach komputerowych, ale w dobrze zaprojektowanej sali wyposażenia są coraz bardziej niepotrzebne. Wreszcie, upewnij się, że masz dostępne systemy oddymiania, aby szybko usunąć obszary dymu. Większość straży pożarnej ma przenośne wentylatory przedmuchowe z długimi tkaninowymi i drucianymi wężami umożliwiającymi dostęp na zewnątrz. Nie pozwalaj nikomu używać respiratora lub aparatu do oddychania, chyba że jest to zatwierdzone do tego celu i nie zostało odpowiednio dopasowane do przeszkolonej osoby.

ŁAGODZENIE SZCZEGÓLNYCH ZAGROŻEŃ

Zanim będzie możliwa dobra ochrona infrastruktury, należy rozważyć kilka innych zagrożeń. Niektóre z tych sytuacji są mało prawdopodobne, ale potencjalnie bardzo kosztowne, jeśli kiedykolwiek wystąpią.

Zapobieganie podsłuchom i pluskwom

Większość podsłuchów jest umieszczana w punktach połączeń przewodów. Wrażliwe miejsca znajdują się w pomieszczeniach sprzętowych, szafach z okablowaniem, skrzynkach połączeniowych, blokach okablowania lub gniazdach danych. Przewód odgałęzienia może być światłowodowy lub koncentryczny lub wykorzystywać parę nieużywanych przewodników wewnątrz istniejącego kabla. Prawdopodobnie będzie to mały przewód, który jest ledwo zauważalny i biegnie do niepozornego miejsca, gdzie może odbywać się monitorowanie i nagrywanie. Po przeniesieniu w bezpieczne miejsce dane można pobrać telefonicznie, bezprzewodowo, przez Internet lub ręcznie. Nagrane dane mogą być nawet kodowane i przechowywane we własnej sieci ofiary. Błędy wideo i / lub audio używane do szpiegowania są podobne do podsłuchów, ponieważ po monitorowaniu danych należy je następnie wysłać w inne miejsce w celu odzyskania. O ile wszystkie dane systemowe nie są zaszyfrowane, w tym wszystkie dane, głos i ruch wideo, ochrona przed podsłuchami musi być silna, ponieważ wykrycie jest w najlepszym przypadku trudne. Najpierw określ, które kable są krytyczne, i sprawdź cały przebieg kabli. Wszystkie kable powinny znajdować się wewnątrz metalowego kanału. Kable do transmisji danych i zasilania powinny wyglądać podobnie i bez oznaczeń ani etykiet z wyjątkiem kodów alfanumerycznych. Krytyczne kanały powinny być tak niepozorne, jak to tylko możliwe, z dala od miejsc, do których mogą mieć dostęp ludzie. Musi istnieć silna kontrola dostępu, alarmy włamaniowe, czujniki ruchu lub monitoring, w którym można uzyskać dostęp do zakończeń, złączy lub przewodów. Krytyczne ciągi kablowe muszą być chronione na całej długości. Kable do transmisji danych między biurkiem a

gniazdkami ściennymi lub podłogowymi są potencjalnymi miejscami podsłuchu. Zagrożone mogą być również kable, wiązki i złącza w systemach mebli biurowych. Dość dobra ochrona jest możliwa dzięki starannemu projektowi, urządzeniom, które zabezpieczają okablowanie danych przed możliwością podsłuchu i wykrywają odłączenie lub manipulację przy jakichkolwiek przewodach danych. Aby zapewnić ciągłą ochronę przed podsłuchami i błędami, nawet gdy wszystkie dane są w pełni zaszyfrowane, należy przeprowadzać okresowe i dokładne inspekcje wizualne, przeszukiwać w celu wykrycia wszelkich nietypowych transmisji o częstotliwości radiowej oraz uważnie testować okablowanie w celu określenia wszelkich anomalii. Wszystko, co zostało zrobione, należy rejestrować i szybko analizować. Niestety, większość szpiegów nigdy nie jest wykrywana i może być kontynuowana niezauważona przez sprawców

Zdalne urządzenia szpiegowskie

Istnieją bardzo czułe odbiorniki radiowe, które mogą monitorować dane systemu informacyjnego przez ściany lub z zewnątrz budynku bez użycia wewnętrznego błędu lub podsłuchu. Urządzenia te mogą po prostu słuchać danych z daleka. Taki sprzęt nie jest publicznie dostępny i jest daleko poza zasięgiem wszystkich szpiegów oprócz najlepiej finansowanych. Jednak obecnie w użyciu jest wiele takich systemów, a znacznie więcej będzie dostępnych wraz ze spadkiem cen. Każda organizacja, której dane są bardzo cenne, jest potencjalnym celem. Najlepszą ochroną jest dobre ekranowanie wokół pomieszczeń ze sprzętem i grubościenny metalowy kanał kablowy dla kabli danych, a wszystko musi być odpowiednio uziemione. Istnieją również nadajniki zakłóceń, które mogą pomóc; te emitują biały szum, który może przytłoczyć sygnały emitowane z infrastruktury IS.

Bomby, groźby, przemoc i ataki

Gwałtowne wydarzenia są nieprzewidywalne i potencjalnie niszczące. To nie są wypadki, ale celowe ataki, mające na celu zakłócenie, spowodowanie szkód i szerzenie strachu. Tragiczne ataki z 11 września i ich następstwa dowiodły wrażliwości ludzi i ich infrastruktury. Luki nadal istnieją, a ryzyko jest jeszcze większe. Skuteczne odstraszanie i łagodzenie skutków staje się wówczas kwestią wzmocnienia ochrony opisanej w tym rozdziale, co nie musi być bardzo kosztowne, biorąc pod uwagę reakcję i odbudowę koszty, które w przeciwnym razie mogłyby wyniknąć. Pomieszczenia lub bezpieczeństwo korporacyjne muszą radzić sobie z większością zagrożeń przemocą, ale infrastruktura wymaga specjalnych zabezpieczeń, aby uniknąć zakłóceń i złagodzić przestoje i konsekwencje finansowe każdego takiego zdarzenia. Rozsądnie dobre środki ochrony i łagodzenia mogą być proste i niedrogie. Stanowe i regionalne oddziały bombowe lub jednostki wybuchowe mogą doradzać i pomagać na wiele sposobów, w tym na bieżących odprawach. Broń masowego rażenia (BMR), inna niż broń jądrowa, szybko staje się realnym zagrożeniem, zwłaszcza że wiele takich urządzeń jest małych i można je łatwo ukryć. Broń masowego rażenia obejmuje środki chemiczne i biologiczne oraz urządzenia zapalające, a nawet niewielkie ilości materiałów radioaktywnych wyrzuconych przez wybuchową brudną bombę mogą wywołać panikę. Rząd uważa te urządzenia za bardzo poważne zagrożenie, a potencjalnym celem są firmy i ich infrastruktura. Nowa przestrzeń biurowa musi mieć teraz certyfikat odporności na bomby, aby eksplozja lub uderzenie bomby ciężarówki nie mogło zawalić budynku. Urzędnicy mogą zazwyczaj przedstawić aktualne informacje o zagrożeniach i zasugerować środki ochronne. Chociaż małe obszary mogą zostać zniszczone, konstrukcja nie zawali się. Podobnie jak niektóre możliwe zagrożenia, istnieją również skuteczne urządzenia ochronne, o których nie można wspomnieć. Nie są one sprzedawane publicznie i dlatego nie są znane dealerom, odsprzedawcom ani dystrybutorom. Koszty mogą być rozsądne, ponieważ są sprzedawane tylko bezpośrednio. Programiści mogą dostarczać niejawne systemy do użytku wojskowego lub rządowego oraz oferować odtajnione wersje innym wybranym użytkownikom. W ten sposób programiści mogą ograniczyć wiedzę o swoich produktach do jak najmniejszej liczby osób, tak aby inni nie mogli odkryć, jak je rozpoznać lub obejść.

Wielu konsultantów, którzy pracowali dla finansowych, regulowanych lub bardzo dużych prywatnych firm, zna niektórych z tych wyspecjalizowanych dostawców. Zwykle konsultant podchodzi do dostawcy i omawia potrzeby; sprzedawca może wówczas skontaktować się bezpośrednio z klientem. Wreszcie, biorąc pod uwagę dzisiejsze środowisko przemocy, poznaj kluczowych lokalnych, stanowych i federalnych organów ścigania oraz funkcjonariuszy śledczych i zapytaj ich, jak najlepiej chronić organizację.

Nagłe wypadki medyczne

Łagodzenie nagłych przypadków medycznych wymaga pomieszczenia pierwszej pomocy na terenie obiektu, pierwszej pomocy i pewnych środków medycznych, jeśli to możliwe, zarejestrowanej pielęgniarki oraz wielu pracowników przeszkolonych w zakresie udzielania pierwszej pomocy i resuscytacji krążeniowo-oddechowej (CPR). Cały personel ochrony i strażnicy powinni posiadać certyfikaty w zakresie udzielania pierwszej pomocy i RKO. Automatyczny defibrylator zewnętrzny (AED) na miejscu uratuje życie i może być obsługiwany przez każdego w sytuacji awaryjnej. Przenośny defibrylator AED kosztuje obecnie około 1000 USD, a sugerowane szkolenie jest niedrogie. AED jest teraz wymagany we wszystkich budynkach zarządzanych przez władze federalne. Wiele centrów handlowych, miejsc zgromadzeń publicznych i komercyjnych samolotów jest obecnie wyposażonych w jedną lub więcej jednostek. Tlen jest często niezbędny do ratowania życia i zapobiegania trwałej niepełnosprawności. Większość ośrodków wyposażonych w AED ma również jednostki tlenowe. Dobre przenośne jednostki kosztują 800 USD lub mniej.

ZAKOŃCZENIE PROCESU PLANOWANIA BEZPIECZEŃSTWA

Ostatni krok niezbędny do ochrony infrastruktury informatycznej składa się z czterech komponentów. Bez dokładnego wykonania któregokolwiek z tych elementów dobre zabezpieczenie nie jest możliwe.

1. Opracuj plan łagodzenia wszystkich zagrożeń.

2. Opracuj wszystkie opcje łagodzenia skutków dla każdego zidentyfikowanego zagrożenia i przeprowadź analizę kosztów i korzyści, aby określić, które opcje są najlepsze.

3. Opracuj ogólny plan reagowania w zakresie bezpieczeństwa, aby pokazać, kto jest za co odpowiedzialny.

4. Wykonaj niezbędne procedury wdrażania, rozliczalności i działań następczych

Plan łagodzenia wszystkich zagrożeń.

FEMA zapewnia obszerne zasoby do planowania łagodzenia zagrożeń wielozagrożeniowych, obejmujące szeroki zakres tematów, w tym aktualizacje e-mailowe. W tym ostatnim kroku pomocne mogą być przewodniki po stanowym i lokalnym planowaniu działań łagodzących skutki.

* Publikacja FEMA 386-1, Pierwsze kroki: Budowanie wsparcia dla planowania łagodzenia skutków, określa proces ograniczania zagrożeń.

* Publikacja 386-2, Zrozumieć swoje ryzyko: identyfikacja zagrożeń i szacowanie strat, przedstawia metodę szacowania kosztów potencjalnych strat spowodowanych powodzią przy użyciu tabel, a nie obliczeń. Te tabele szybko pokazują, że straty mogą być znacznie większe niż oczekiwano.

* Publikacja 386-3 „Opracowanie planu łagodzenia skutków: identyfikacja działań łagodzących i strategii wdrażania” zawiera wytyczne dotyczące opracowywania strategii łagodzenia skutków.

* Publikacja 386-4, Bringing the Plan to Life: Implementing the Hazard Mitigation Plan, omawia wytyczne dotyczące wdrażania.

* Publikacja 386-5, Korzystanie z przeglądu korzyści i kosztów w planowaniu łagodzenia skutków, zawiera heurystykę wyboru opcji łagodzenia w celu maksymalizacji opłacalności wydatków

* Publikacja 386-6 „Integrating Historic Property and Cultural Resources Considerations to Hazard Mitigation Planning", omawia, jak współpracować z lokalnymi władzami planistycznymi w celu ochrony kapitału kulturowego.

* Publikacja 386-7 „Integracja zagrożeń spowodowanych przez człowieka z planowaniem łagodzenia skutków" omawia jak planować ataki terrorystyczne lub przestępcze w planowaniu awaryjnym

* Publikacja 386-8, Multi-Jurisdictional Mitigation Planning, podkreśla znaczenie wspólnego planowania reagowania (Federalna Agencja Zarządzania Kryzysowego 2006).

Gdy wszystkie możliwe sytuacje zagrożenia zostaną zidentyfikowane i ocenione zgodnie z opisem we wcześniejszej części, następnym krokiem jest opracowanie jak największej liczby opcji zapobiegania, powstrzymywania lub łagodzenia zakłóceń, obrażeń lub szkód wynikających z każdego zagrożenia. Chociaż niektórym zagrożeniom nie można zapobiec, zawsze istnieją sposoby na przygotowanie się i złagodzenie ich skutków. Zwykle istnieje wiele opcji łagodzenia skutków, więc celem jest określenie, które opcje są najbardziej praktyczne i niedrogie. Jedynym obiektywnym sposobem osiągnięcia tego jest analiza kosztów i korzyści. W rzeczywistości opcje ochrony przed wieloma różnymi zagrożeniami będą podobne, ale każdą opcję należy zachować, dopóki nie zostanie określona najlepsza strategia łagodzenia skutków dla każdego zagrożenia. Tutaj również prawdopodobnie istnieje jedna wspólna strategia łagodzenia skutków wielu różnych zagrożeń. Wszystkie wiarygodne zagrożenia powinny zostać wymienione w planie łagodzenia skutków, ale przedstawionych projektów łagodzących będzie znacznie mniej. Po zakończeniu następnego kroku można ukończyć plan łagodzenia wszystkich zagrożeń. Instrukcje obsługi FEMA 386 opisane powyżej zawierają sugerowany format i zawartość. Poradnik nr 9 FEMA (FEMA 386-9), zatytułowany Korzystanie z planu łagodzenia zagrożeń do przygotowania udanych projektów łagodzenia skutków, jest obszernym przewodnikiem po korzystaniu ze wszystkich innych zasobów wymienionych powyżej. Kompletny plan łagodzenia skutków powinien być przeznaczony wyłącznie do użytku oficjalnego i nie powinien być udostępniony z wyjątkiem osób, które muszą znać te informacje. Kompletny plan byłby bardzo pomocny dla potencjalnego wichrzyciela, ponieważ pokazuje, gdzie organizacja jest narażona i na jakie zagrożenia. Jeśli ujawnienie całego planu nie jest dobrze kontrolowane, jego zawartość może zostać ujawniona, wyłudzona lub sprzedana przez osobę mającą dostęp do informacji poufnych. Jednak streszczenie planu i skrócone ustalenia powinny być szeroko rozpowszechniane, aby wszyscy interesariusze wiedzieli, że wiele się robi, aby je chronić.

Analiza kosztów i korzyści

Bezpieczeństwo jest bezcelowe, o ile nie jest opłacalne, a także wartościowe: to znaczy, że koszt łagodzenia każdego zagrożenia musi być niższy niż potencjalne korzyści i oszczędności wynikające z nie zajścia zdarzenia, ponieważ ochrona jest skuteczna. Koszty każdej opcji można łatwo określić; są to koszty początkowe i bieżące. Jednak niektóre przyszłe korzyści będą niematerialne i wszystkie trzeba będzie w przybliżeniu. Długoterminowe korzyści wynikające z braku wydarzeń muszą odzwierciedlać przybliżone koszty:

* Zakłócenia, które mogłyby zmniejszyć produktywność firmy i wydajność jej systemów informatycznych

* Morale i wydajność, które mogą gwałtownie spaść i pozostać na bardzo niskim poziomie, ponieważ ludzie czują się zagrożeni i pozbawieni ochrony

* Utrata biznesu lub klientów do czasu przywrócenia normalnej działalności

* Koszty reakcji i zwrotu kosztów, w tym dodatkowy czas i nadgodziny, wydatki, w tym zakwaterowanie i posiłki, tymczasowe udogodnienia, relacje publiczne i koszty obrony prawnej, które prawdopodobnie zostaną poniesione

* Usługi prawne, public relations i inne usługi i wydatki w celu naprawienia szkód reputacyjnych i spadku ceny akcji oraz przywrócenia dobrej woli

Nie wszystkie te koszty będą towarzyszyć każdemu zagrożeniu. Ale z drugiej strony mogą również wystąpić dodatkowe, nieoczekiwane koszty. Ogólnie rzecz biorąc, koszty reagowania i odzyskiwania wszelkich poważnych zdarzeń związanych z bezpieczeństwem są zwykle znacznie wyższe niż oczekiwano. Niemniej jednak każdą sytuację można zbadać i określić niektóre koszty, aby ułatwić statystycznie ważną analizę kosztów i korzyści. Informacje o kosztach i korzyściach nie mają znaczenia, chyba że każda z nich jest powiązana ze wspólnym przedziałem czasowym. Prawdopodobieństwo każdego zagrożenia należy oceniać w ujęciu rocznym, tak aby zarówno koszty łagodzenia, jak i potencjalne korzyści mogły zostać zamortyzowane w tym samym cyklu życia. Istnieje wiele metod analizy wartości kosztów i większość z nich wykracza poza zakres tego rozdziału. Jednak dla tych, którzy nie są przeszkoleni finansowo, rząd federalny ma dobry system, ogólnie dostępny, który jest powszechnie wymagany w rządzie. Rząd USA nazywa ten system BCA, co oznacza analizę korzyści i kosztów. W ramach tego systemu FEMA opracowała narzędzie analizy kosztów i korzyści, które pomaga wnioskodawcom w przeprowadzaniu analiz finansowych, takich jak wartość bieżąca netto. Ta sama strona zawiera dane o zagrożeniach. Szczególną zaletą systemu BCA jest to, że OMB publikuje aktualne dane dotyczące kosztów funduszy, potrzebne do prognozowania wszelkich kosztów. Niektóre z modeli prywatnych mają tendencję do stosowania szalenie optymistycznych (lub rażąco nieaktualnych) przyszłych stóp procentowych, co unieważnia sensowne wyniki. Ponownie, rozsądnie jest zastosować model rządu federalnego po prostu jako kwestia unikania ryzyka. Model BCA jest szeroko stosowany i wymagany w przypadku wielu wniosków o dotacje.

Plan reagowania na zagrożenia

Plan łagodzenia zagrożeń jest potrzebny do udokumentowania oceny zagrożenia i wyszczególnienia opcji łagodzenia oraz przewidywanych kosztów i korzyści związanych z każdym z nich; potrzebny jest również plan reagowania w zakresie bezpieczeństwa, aby kierować każdą z zainteresowanych stron zgodnie z rodzajem napotkanego zagrożenia. Celem planu reagowania w zakresie bezpieczeństwa jest jasne określenie, kto jest odpowiedzialny i kto zrobi co, kiedy i jak, kiedy pojawi się jakiekolwiek zagrożenie. Nowy format NRF zmienia i przywraca koncepcję funkcji wsparcia w sytuacjach kryzysowych (EFS) dla każdego działania wspierającego, którego każda organizacja może potrzebować. Obecnie istnieje 16 ponumerowanych EFS, zaczynając od EFS-1, „Transport", ESF-2, „Komunikacja i alarmowanie", a kończąc na EFS-16, „Zdrowie zwierząt". Zaleca się zachowanie standardowych tytułów EFS, nawet jeśli wiele z nich może nie mieć zastosowania do organizacji pozarządowych, choćby po to, by zachować jednolitość i język, który wszyscy rozumieją. Aby uzyskać skuteczną reakcję, potrzebne będą dodatkowe EFS, ale należy je policzyć na 17 i więcej. Jedną z przydatnych szybkich informacji w nowym formacie planu reagowania jest macierz przypisania funkcji wsparcia awaryjnego, jednostronicowa grafika pokazująca, która agencja lub departament jest odpowiedzialny za podstawowe, dodatkowe lub pomocnicze obowiązki dla każdego EFS. Jest to przydatny przewodnik dla kierownictwa i personelu w przypadku problemów. Gdy plan reagowania jest gotowy, każdy dział, którego to dotyczy, powinien napisać standardowe procedury operacyjne, aby nakreślić procedury,

których będzie używał do reagowania. Termin ten jest podawany w cudzysłowie, ponieważ są one zwykle podawane jako wskazówki, aby zapewnić pewną elastyczność w dostosowaniu się do rzeczywistych warunków. Wymóg sztywnego przestrzegania procedury jest zaproszeniem do postępowania sądowego. Kompletny plan reagowania w zakresie bezpieczeństwa powinien być również przeznaczony wyłącznie do użytku oficjalnego i udostępniony tylko tym, którzy muszą wiedzieć. W końcu ten plan pokazuje kłopotliwym, jak zareaguje organizacja. Jednak komunikat prasowy podsumowujący plan powinien być szeroko rozpowszechniany, aby wszyscy interesariusze wiedzieli, że organizacja stara się ich chronić.

Wdrożenie, odpowiedzialność i dalsze działania

Gdy wszystkie plany zostaną ukończone i zatwierdzone przez kierownictwo i kluczowych urzędników, rozpoczyna się realizacja. Ze wspomnianych wcześniej poradników pomocnych będzie FEMA 386-4, Bringing the Plan to Life. Ten pierwszy krok implementacji jest najbardziej krytyczny dla procesu ochrony bezpieczeństwa. Rozpoczyna się od szkolenia, aby wszyscy zaangażowani zrozumieli i zaakceptowali procedury. Następnie muszą odbywać się okresowe ćwiczenia i ćwiczenia, aby przetestować plan reagowania i potwierdzić, że szkolenie było skuteczne. Plany, które nie są okresowo testowane, szybko się zapomina. Każde ćwiczenie i ćwiczenie należy przeanalizować, aby określić, co poszło dobrze, a co ważniejsze, co nie, i jak zrobić to lepiej w przyszłości. Dlatego też każda reakcja awaryjna powinna zostać poddana przeglądowi. Ważna jest dokumentacja przed, w trakcie i po wydarzeniu. Z każdego wydarzenia wyciągniemy pewne wnioski, które należy wykorzystać do aktualizacji i ulepszania systemów bezpieczeństwa, aby działały lepiej w przyszłości. Niezwykle ważne jest również ustalenie odpowiedzialności za bezpieczeństwo infrastruktury. Za każdą funkcję powinna odpowiadać tylko jedna osoba. Odpowiedzialności nie można rozłożyć na kierownictwo lub działy, ani też nie można jej nosić jako drugiej czapki dla kogoś, kto ma wiele innych obowiązków. Wyższa odpowiedzialna władza musi ustalić harmonogramy okresowych przeglądów i aktualizacji planów i procedur, szkoleń i ćwiczeń, aby upewnić się, że program ochrony pozostaje aktualny i skuteczny. Dobre zarządzanie bezpieczeństwem musi również obejmować nadzór. Dobre planowanie musi rozpocząć się w sali konferencyjnej, a dyrektorzy muszą również zapewniać stały nadzór, aby zapewnić dobre bezpieczeństwo. Zewnętrzni, niezależni audytorzy kierowani z sali konferencyjnej najlepiej sprawdzają aktualny stan programu bezpieczeństwa. Pisemna opinia biegłego rewidenta jest dowodem na to, czy organizacja w pełni przestrzega przepisów. Aby zachować spokój kierownictwa (i być może jako wymóg utrzymania ubezpieczenia i uzyskania kredytu), mogą być przeprowadzane okresowe kontrole bezpieczeństwa, testowanie zabezpieczeń i niektóre testy penetracyjne, w tym oszustwa w celu uzyskania dostępu wykonane przez niezależnych specjalistów.