ZAGROŻENIA FIZYCZNE W INFRASTRUKTURZE INFORMATYCZNEJ

WPROWADZENIE.

W tej części opiszemy szeroki zakres możliwych zagrożeń fizycznych, które mogą wpłynąć na infrastrukturę systemów informatycznych (IS). Zagrożeniem jest każda wiarygodna sytuacja - faktyczna, nieuchronna, przewidywana lub możliwa - z możliwością wyrządzenia szkody, uszkodzenia lub zakłócenia. Terminy zagrożenie i zagrożenie są używane w tej części synonimicznie i mają to samo znaczenie. Ryzyko odnosi się do prawdopodobieństwa wystąpienia zagrożenia. Zagrożona infrastruktura może być dowolnym elementem systemu komputerowego lub sieci komunikacyjnej; którykolwiek z kabli, przewodów lub urządzeń, które przenoszą moc lub dane; lub dowolne z usług wsparcia lub narzędzi potrzebnych do utrzymania pełnej wydajności IS. Ponadto zagrożenia dla pracowników stanowią istotny element bezpieczeństwa fizycznego. Szybkość i dokładność każdego systemu zależy od wydajności długiego łańcucha komponentów fizycznych, a także od wydajności wszystkich osób, które używają lub konserwują każdy komponent. Coś mniej niż pełna wydajność całego systemu może być kosztowna. Zagrożeniem fizycznym jest każde zdarzenie, które może obniżyć wydajność systemu informatycznego - niezależnie od tego, czy takie zdarzenie rzeczywiście występuje lub jest nieuchronne, czy jest prawdopodobne prawdopodobne lub możliwe, czy też całkowicie nieoczekiwane i bez ostrzeżenia. Lista możliwych zagrożeń jest długa, zaczynając od naturalnych i spowodowanych przez człowieka zewnętrznych zdarzeń, które mogą obniżyć wydajność IS. Wiele innych możliwych zagrożeń jest wewnętrznych, wynikających z wypadków, niewłaściwego użycia lub umyślnego ataku. Zagrożenia wewnętrzne obejmują również awarie niezawodności, problemy z instalacją lub konserwacją lub brak odpowiednich testów. Zagrożenia mogą być również spowodowane sytuacjami wewnątrz obiektu, budynku lub kompleksu, lub w wyniku lokalnych lub regionalnych wydarzeń lub, coraz częściej, wydarzeń na całym świecie, a nawet z kosmosu. Zagrożenia zdarzają się i mogą pochodzić z niemal dowolnego miejsca, dlatego rozważenie wszystkich prawdopodobnych i znaczących zagrożeń jest rozsądne i o wiele tańsze. Chociaż terminologia często odnosi się do „wszystkich możliwych zagrożeń", czytelnicy muszą zrozumieć dorozumiane założenie, że rozważają tylko uzasadnione kategorie zagrożeń. Planowanie radzenia sobie z skutkami niszczącego świat zderzenia z asteroidą wielkości kontynentu jest bezużyteczne; próba zdefiniowania strategii reagowania na atak kosmicznych najeźdźców uzbrojonych w karabiny jest niemożliwa i bezużyteczna. Ta część rozpoczyna proces oceny zagrożenia, który rozpoczyna się od zidentyfikowania wszystkich uzasadnionych sytuacji zagrożenia. Proces ten musi być kompleksowy i rygorystyczny oraz obejmować wszystkie zainteresowane strony. Nie wystarczy po prostu przypisać prawdopodobieństwo i wpływ na zwykłe lub oczywiste zagrożenia. Musi zostać przeprowadzona pełna analiza ryzyka, aby ryzyko, podatność na zagrożenia oraz koszty reakcji i odzyskiwania można było zmierzyć.W przeciwnym razie cały proces jest bezwartościowy. W przypadku braku kompleksowego planowania bezpieczeństwo staje się nieracjonalnym wyborem dostawców i rozwiązań, które mogą jedynie zwiększać koszty i zwiększać ryzyko odpowiedzialności. Alternatywnie, strategiczny proces zarządzania ryzykiem może zmaksymalizować przyszłe zyski i zwiększyć wartość dodaną, chronić morale i wydajność, zwiększać wartość firmy i poprawiać relacje z klientami i społecznościami.

Wydarzenia z 11 września 2001 r. Wywołały wstrząsające wezwanie, że mogą się zdarzyć nieoczekiwane zagrożenia, a nawet najlepsze praktyki bezpieczeństwa, produkty i usługi mają niewielką wartość bez odpowiedniego planowania, wdrażania i wsparcia. Huragan Katrina, cztery lata później w 2005 r., Po raz kolejny pokazał, że zarówno biznes, jak i rząd są wciąż nieprzygotowane, mimo że takie zdarzenie było przewidywane wiele razy. Ten rozdział sugeruje kompleksowe spojrzenie na bezpieczeństwo fizyczne, które może wnieść wartość dodaną i pomóc w zapobieganiu katastrofie.

KONTEKST I PERSPEKTYWA.

Dane historyczne i statystyki mają ograniczoną wartość w przewidywaniu przyszłych zagrożeń.. Przeszłość nie jest już prologiem, ponieważ powstaje wiele nowych zagrożeń, a wiele rodzajów incydentów jest coraz poważniejszych, powszechnych, złożonych, niszczących i kosztownych. Proliferujące i coraz bardziej rozproszone elementy systemu infrastruktury są często wrażliwe i trudne do ochrony. A hybrydowe konfiguracje nowych i starszych systemów znacznie komplikują proces ochrony. Istnieje kilka statystyk zagrożeń, które mogą wiarygodnie prognozować przyszłość infrastruktury. Raporty dotyczące przestępstw komputerowych dotyczą głównie bezpieczeństwa logicznego, podczas gdy ogólne statystyki dotyczące przestępstw często nie odnoszą się bezpośrednio do bezpieczeństwa komputerowego. Informacje historyczne są dodatkowo wadliwe, ponieważ wiele incydentów nigdy nie jest wykrywanych, a znacznie więcej nie zgłaszane z obawy przed zawstydzeniem, odpowiedzialnością lub utratą działalności. Wiele incydentów związanych z bezpieczeństwem jest maskowanych jako problemy kontroli jakości z tych samych powodów lub błędnie zdiagnozowanych, ponieważ nikt nie miał czasu na ustalenie prawdziwych przyczyn. Brak wiarygodnych precedensów, przewidywanie przyszłe zagrożenia są szczególnie trudne - ale coraz bardziej konieczne. Większość incydentów zdarza się nagle, bez ostrzeżenia, i często tam, gdzie są najmniej oczekiwane. Wiele zagrożeń, które kiedyś uważano za mało prawdopodobne, obecnie występuje szeroko i uderza z zaskakującą intensywnością i dewastacją. Do innych czynników przyczyniających się należy słabe zarządzanie ryzykiem z powodu braku doświadczenia, odmowy lub samozadowolenia, które mogą szybko przekształcić rutynowe zagrożenia w kosztowne incydenty. Firmy o dobrej gotowości bezpieczeństwa zwykle mogą przetrwać, podczas gdy wiele innych nie

Dzisiejsze ryzyko jest większe.

Dzisiejsze zagrożenia są coraz bardziej wyrafinowane, nieprzewidywalne, potencjalnie poważne i coraz bardziej powszechne. Incydenty destrukcyjne mogą wynikać z błędów lub wypadków, szpiegów lub hakowania, wandalizmu, niezadowolonych lub zakłócających spokój osób, sporów pracowniczych, demonstracji, niepokojów społecznych, ekstremistów z wielu stron oraz, w coraz większym stopniu, terroryzmu krajowego i międzynarodowego. Chociaż w ostatnich latach liczba przestępstw z użyciem przemocy spadła w niektórych częściach świata, dane te mogą wprowadzać w błąd, ponieważ rzadko obejmują wydarzenia związane z miejscem pracy. Przemoc w miejscu pracy jest teraz powszechna i często bez ostrzeżenia. Incydenty mogą obejmować nękanie, straszenie bombami, napady, sytuacje zakładników, strzelanie lub podpalenie. I każde z tych zagrożeń może poważnie wpłynąć na wydajność SI. Zagrożenia fizyczne mogą wykraczać poza bezpośrednie ataki. Wiele strachów nie prowadzi do faktycznej przemocy, a incydenty zakłócające mogą zdarzyć się poza miejscem pracy. Jednak niezależnie od miejsca zdarzenia związane z przemocą stają się coraz bardziej powszechne, destrukcyjne i kosztowne. Ci, którzy zagrażają infrastrukturze IS, muszą przynajmniej uzyskać dostęp do jej fizycznej części, ale często można to zrobić w sposób niepozorny, przez oszustwo, oszustwo lub po prostu przymusowe wejście. Fizyczny atak może być najlepszym sposobem na skompromitowanie systemu informatycznego - znacznie bardziej skuteczny i rzadziej wykrywalny niż atak logiczny. Często wiele istotnych elementów systemu jest wrażliwych, narażonych lub łatwo dostępnych. Składniki te obejmują okablowanie i kable, punkty połączeń i połączeń, sprzęt systemowy i sieciowy oraz narzędzia, które je obsługują. Ataki fizyczne lub szpiegowanie za pomocą środków fizycznych są często łatwe, szybkie, bezpieczne i pewne.

Prawdopodobne cele.

Firmy i organizacje są coraz bardziej prawdopodobne ,ze będą celem hakerów, niezadowolonych pracowników, konkurencji, zwalnianych osób, demonstrantów, grup nienawiści, ekstremistów, a nawet terrorystów. Motywy mogą obejmować rzucający się w oczy, kuszący lub rzucający wyzwanie cel, wściekłość lub zemstę, okazję do wyrządzenia szkody w reputacji lub przynajmniej negatywny

rozgłos, złożenie oświadczenia politycznego, wymuszenie lub szantaż, lub dla osobistych korzyści lub zysków. Często nie ma dostrzegalnych motywów. Poza tym, że są prawdopodobnymi celami, większość firm jest również wygodnymi, łatwymi i bezpiecznymi celami, ponieważ większość z nich jest nieświadoma i nieprzygotowana na dzisiejsze zagrożenia, a tym bardziej na przyszłe. Chociaż obiekty rządowe pozostają preferowanymi celami, wiele z nich jest teraz lepiej chronionych niż większość firm. Kolejne prawdopodobne zagrożenie wynika z potrzeby ekstremistów i terrorystów do finansowania ich działalności. Wiele grup i wszystkie niezależne, samokierujące się komórki są uzależnione od przestępczości w celu finansowania swoich działań. Dzisiejsze przestępstwa mogą obejmować rabunek i zatrzymania, fałszywe waluty i karty kredytowe, phishing i oszustwa internetowe, kradzież, wymuszenia, szantaż oraz sprzedaż pirackiego oprogramowania i inne podróbki. Ponadto wiele zagranicznych rządów, przedsiębiorstw i organizacji przestępczych aktywnie uczestniczy w szpiegowaniu. Chociaż są to głównie problemy z bezpieczeństwem korporacyjnym i logiczne, stanowią one również potencjalne zagrożenia fizyczne, których należy powstrzymać.

Problemy z produktywnością.

Dobre bezpieczeństwo może być bezpośrednio skorelowane z wysoką produktywnością, co z kolei może poprawić wydajność, zadowolenie klientów i dobrą reputację. Dobre bezpieczeństwo jest mierzalne i może strategicznie wzmocnić każdy z tych czynników, dodając zarówno wartość, jak i zysk. Coś mniej niż dobre bezpieczeństwo zachęca do marnowania czasu i pieniędzy. Ludzie, którzy nie czują się bezpiecznie, nie będą produktywni. Dotyczy to pracowników, odwiedzających, dostawców i innych osób w siedzibie, a także klientów, dostawców, akcjonariuszy i innych interesariuszy w odległych lokalizacjach. Każdy, kto korzysta z dowolnego systemu informatycznego, musi mieć pewność, że bezpieczeństwo fizyczne i prywatność są ubezpieczone, a system jest nieprzerwany, bezpieczny i działa z pełną wydajnością. Każdy zainteresowany musi brać udział w procesie planowania, ogólnie rozumieć zagrożenia i wspierać je oraz wspierać procedury bezpieczeństwa. W przeciwnym razie wydajność nieuchronnie ucierpi. Ilekroć zdarzy się incydent bezpieczeństwa, morale i wydajność prawdopodobnie spadną i mogą pozostawać niskie przez wiele tygodni, a nawet miesięcy. Niezależnie od tego, czy infrastruktura zostanie naruszona, czy nie, prawdopodobne jest znaczne zakłócenie działalności. Nawet gdy nie ma obrażeń ani szkód, postrzeganie potencjalnego zdarzenia może być kosztowne; może zakłócać produktywność, tracić biznes i klientów oraz zagrażać dobremu wizerunkowi. Nikt nie wie, jak często występują zdarzenia związane z produktywnością. Firmy na ogół ich nie zgłaszają, podobnie jak media. Ale te rzeczy się zdarzają i prawdopodobnie ze znaczną częstotliwością. Jednak wszystkim zagrożeniom można w pewnym stopniu złagodzić, a wielu bardziej można zapobiegać przy znacznie niższych kosztach niż konsekwencje dzięki skutecznym przygotowaniom technicznym, odpowiedniej świadomości pracowników i szkoleniom oraz dobrze zaplanowanym i dobrze przećwiczonym reakcjom.

Terroryzm i przemoc są teraz poważnymi zagrożeniami.

Akty terroryzmu i przemocy są teraz rzeczywistością, która może wystąpić w dowolnym miejscu na świecie. 11 września 2001 r. I wydarzenia, które nastąpiły po tym wydarzeniu, uświadomiły sobie surową rzeczywistość, że przemoc może się zdarzyć wszędzie i może spowodować ogromne szkody i zakłócenia. A większość poważnych katastrof może zakłócać systemy informacyjne dalekie od faktycznych incydentów. Przemoc w miejscu pracy ma również miejsce coraz częściej i często w obiektach uważanych za bezpieczne. Coraz częściej zdarzają się bomby i przerażenia biologiczne lub chemiczne, groźby osobiste, nękanie, sytuacje zakładników i strzelaniny. Niezależnie od tego, czy występuje rzeczywista przemoc, czy same zagrożenia, wiele generowanych plotek i wyobrażona bliskość niebezpieczeństwa to wszystkie zdarzenia związane z produktywnością, które mogą poważnie zakłócać działanie systemów informatycznych przez długi czas. W związku z tym stają się one

problemami bezpieczeństwa infrastruktury, które wymagają specjalnego planowania i nie należy ich pozostawiać pracownikom ochrony lokali w celu zapobiegania. Istnieją inne poważne zagrożenia ze strony wywiadu zagranicznego, terrorystów i grup krajowych ogólnie nieznanych opinii publicznej. Niektóre z nich zostały dobrze wyjaśnione w raporcie Project Megiddo opublikowanym przez Federalne Biuro Śledcze (FBI) w 1999 roku w oczekiwaniu na tysiąclecie. Raport zawiera „strategiczną ocenę FBI dotyczącą potencjału terroryzmu wewnętrznego w Stanach Zjednoczonych przeprowadzoną w oczekiwaniu na nowe tysiąclecie lub w odpowiedzi na nie". Przytoczone wówczas zagrożenia są zasadniczo niezmienione, z tym wyjątkiem, że dodano więcej nieznanych wcześniej zagrożeń. Są konsultanci z kontaktami FBI, którzy mogą udzielić cennych porad. Próba przemocy stanowi obecnie poważne zagrożenie dla wszystkich infrastruktur IS. Jednak dokładne planowanie bezpieczeństwa może wiele zrobić, aby uniknąć problemów i niepotrzebnych wydatków.

Koszty uszkodzonej infrastruktury IS.

Bezpośrednie koszty przestoju systemu mogą przekroczyć wiele tysięcy dolarów na godzinę. Straty obejmują luźne koszty osób, które nie mogą korzystać z systemów, koszty wsparcia i utrzymania skierowane do przywracania operacji, koszty odzyskiwania, nadgodziny, a często zakwaterowanie, wyżywienie i koszty podróży podczas odzyskiwania. Zwykle wiele zasobów zewnętrznych jest potrzebnych do reagowania i odzyskiwania. Wszystko szybko staje się drogie. Często, aby dodatkowo zintensyfikować koszty, potrzebne zasoby nie są natychmiast dostępne. Koszty pośrednie mogą być również znaczące. Przywrócenie i utrzymanie dobrych public relations może być kosztowne. Często publiczne ogłoszenia, komunikaty prasowe i briefingi dla mediów informacyjnych i finansowych oraz akcjonariuszy są potrzebne, aby zneutralizować publiczne zawstydzenie i kontrolować plotki. Należy skontaktować się z kluczowymi klientami i upewnić się, a oczekujące zamówienia zostały przesunięte w czasie. Jeszcze większe koszty obejmują utratę działalności lub udziału w rynku oraz spadające ceny akcji. Konkurenci często będą czerpać jak najwięcej korzyści, co wymaga dodatkowych kosztów ochrony marek i reputacji. Dowolna liczba takich kosztów może zniszczyć przedsiębiorstwo, chyba że skuteczne i szybkie wdrożenie silnych środków bezpieczeństwa. Odpowiedzi z reklamami są często katastrofalne. W rzeczywistości awaria infrastruktury na więcej niż kilka godzin jest często śmiertelna, a przedsiębiorstwo nigdy nie może w pełni się zregenerować. Dobre bezpieczeństwo zwykle może zapobiec katastrofalnym kosztom.

Kto musi być zaangażowany.

Wiele zagrożeń dla systemów informatycznych dotyczy także pracowników ochrony korporacji lub pomieszczeń, których zadaniem jest ochrona osób i mienia w miejscu pracy i wokół niego. Zaangażowani są również CEO i CFO, ponieważ muszą oni teraz przestrzegać obowiązujących przepisów ustawowych i wykonawczych. Zgodność wymaga, aby zdarzenia, które mogą mieć istotny wpływ na wyniki finansowe, były uwzględniane w dokumentacji finansowej i oświadczeniach organizacji. Poważne zdarzenia związane z bezpieczeństwem to oczywiście takie zdarzenia, których wpływ należy teraz przewidzieć. Bezpieczeństwo lokali często obejmuje niewiele więcej niż strażników, kontrolę dostępu i pewien nadzór. Ich zrozumienie specjalnych potrzeb bezpieczeństwa infrastruktury IS jest często minimalne, powiązane z ogólnymi procedurami bezpieczeństwa fizycznego i rzadko wykracza poza bezpośrednie przesłanki. Jednak bezpieczeństwo IS wymaga dodatkowej wiedzy, doświadczenia, ochrony i wsparcia. Dobre bezpieczeństwo musi być silne, szybko działające, skoncentrowane na konkretnych celach i ściśle monitorowane. Skuteczne systemy wczesnego ostrzegania są niezbędne, aby zapobiec występowaniu zagrożeń. W rzeczywistości każda funkcja bezpieczeństwa będzie miała własne potrzeby i priorytety oraz będzie korzystać z własnych zasobów. Podczas poważnego incydentu bezpieczeństwo lokali, mieszkańców, systemów informatycznych i infrastruktury musi koordynować sprawnie i skutecznie. Muszą także sprawnie współpracować z

lokalnymi jednostkami straży pożarnej i policji, innymi ratownikami i wieloma zewnętrznymi zasobami. Kto zatem powinien zarządzać procesem określania zagrożeń dla infrastruktury IS? A kim są interesariusze, którzy powinni być zaangażowani w ten proces? Najlepszą osobą do zarządzania fizycznym bezpieczeństwem systemów informatycznych jest ten, kto wie dużo o potencjalnych zagrożeniach i infrastrukturze IS. Kierownik biura, kierownik obiektu lub dyrektor ds. bezpieczeństwa firmy lub ich pracownicy są zwykle wyposażeni w sprzęt do określania bezpieczeństwa IS lub zarządzania nim. Często także dyrektor ds. Informacji (CIO), dyrektor ds. bezpieczeństwa informacji (CISO) i urzędnicy ds. Bezpieczeństwa IS (ISSO) zajmują się ochroną danych i przetwarzaniem danych i nie są najlepszymi osobami do zrozumienia bezpieczeństwa fizycznego IS, szczególnie w duża instalacja. Dlatego najlepsza osoba to zaufana osoba z odpowiednią wiedzą i doświadczeniem oraz wystarczającą ilością czasu, aby dobrze zarządzać procesem. Planowanie i zarządzanie bezpieczeństwem infrastruktury, wdrażanie i testowanie go, szkolenie i zwiększanie świadomości bezpieczeństwa, monitorowanie oraz okresowa aktualizacja systemu i procedur to praca w pełnym wymiarze godzin w większości organizacji i wymaga personelu pomocniczego w większych organizacjach. Rozdział 65 tego podręcznika szczegółowo omawia rolę CISO. Inną kwestią jest to, że nikt nie powinien znać wszystkich tajemnic, co jest zasadą, która stała się szczególnie ważna w postępowaniu z infrastrukturą IS. Kiedy pojawiają się problemy, wielu ekspertów musi mobilizować się bardzo szybko, skutecznie i skutecznie. Aby to zrobić, respondenci muszą znać wszystkie systemy informacyjne i mieć szybki dostęp do infrastruktury. Bez względu na to, jak bardzo zaufano, nikt nie powinien wiedzieć wszystkiego o fizycznej i logicznej obronie. (W razie potrzeby takie informacje powinny być bezpiecznie przechowywane przy użyciu silnej kontroli dostępu.) Rozsądnie jest podzielić sekrety, aby żadna grupa nie znała ani nie miała dostępu do nich wszystkich. Po zrobieniu tego wiele osób może następnie dzielić się każdą częścią tajemnic i obserwować się nawzajem, aby nikt nie był niezbędny. Rozdział 45 tego podręcznika przedstawia szczegóły zarządzania pracownikami i bezpieczeństwa. Ale tylko luki w zabezpieczeniach i implementacje obronne powinny być tajemnicą. Nie ma sensu informowanie innych o mechanizmach obronnych i o tym, gdzie organizacja jest wrażliwa. Jednak proces określania podstawowych zagrożeń powinien być powszechnie znany wśród wszystkich zainteresowanych stron. Identyfikując dużą liczba zagrożeń, które zostały ocenione - ale z zachowaniem tajemnicy prawdopodobieństwa, podatności na zagrożenia i informacji o wpływie - możemy zniechęcić potencjalnych kłopotliwych, przynajmniej przedstawiając pewne pojęcie o liczbie uwzględnionych zagrożeń. Przy odrobinie szczęścia zaatakują mniej przygotowane strony.

Problemy z odpowiedzialnością.

Oprócz potrzeby skutecznego reagowania w sytuacjach kryzysowych, inna kwestia, która staje się coraz ważniejsza, jest potencjalnie bardzo kosztowna i często jest pomijana. To jest kwestia odpowiedzialności. Każda organizacja ma prawny i powierniczy obowiązek ochrony ludzi i mienia w obrębie i wokół swoich pomieszczeń. Jeśli jakiekolwiek obrażenia lub szkody wystąpią w miejscu pracy lub wokół niego - nawet długo po nim - prawdopodobnie pojawią się zarzuty zaniedbania. Motywem jest często to, że odszkodowania zasądzane przez sądy mogą być bardzo duże, a prawnicy często podejmują te sprawy w spekulacjach, mając nadzieję na otrzymanie bardzo wysokich opłat. Niezależnie od tego, czy organizacja rzeczywiście ponosi winę, czy nie, wynikające z niej opłaty prawne, czas i koszty potrzebne do obrony organizacji, zła reklama i możliwa utrata działalności, a także ewentualne kary i nagrody mogą być druzgocące. Jeśli domniemane jest zaniedbanie, problemem jest to, czy organizacja była odpowiednio przygotowana na wypadek awarii i czy jej reakcja była skuteczna. Pytanie jest po prostu: Czy kierownictwo wykonuje swój obowiązek ochrony organizacji? Odpowiedź twierdząca wymagałaby co najmniej:

* Dowodu dokładnego procesu oceny zagrożenia

* Dobrych planów bezpieczeństwa, zasad i procedur, które zostały faktycznie wdrożone

* Odpowiednigo szkolenia i aktualna świadomość bezpieczeństwa

* Okresowe ćwiczenia, ćwiczenia, przeglądy bezpieczeństwa i informacje zwrotne ze znanych wydarzeń

* Okresowe aktualizacje w celu zapewnienia skuteczności bezpieczeństwa

Jeżeli można wykazać, że nie podjęto wszystkich tych środków lub nastąpiły odstępstwa od ogólnie przyjętych norm, wynik może być karny, jak również odszkodowania za szkody. Rażące zaniedbanie prawdopodobnie również będzie zarzucane, w takim przypadku ubezpieczenie może nie bronić oskarżonej organizacji lub osób, które wówczas byłyby osobiście odpowiedzialne. Nawet z obowiązującym ubezpieczeniem, może nie być wystarczające do pokrycia bardzo dużych kar, które są często przyznawane przez jury. Nawet po udzieleniu wszystkich prawidłowych odpowiedzi oskarżeni często uznają ich za winnych, dopóki nie okażą się niewinni. I może to być długi, bolesny i kosztowny proces. Jednak niemal żelazną obroną przed odpowiedzialnością jest przestrzeganie procedur federalnych. Najbardziej kompleksowe z nich pochodzą z Departamentu Bezpieczeństwa Wewnętrznego (DHS) i jego Federalnej Agencji Zarządzania Kryzysowego (FEMA). Spośród wszystkich innych procedur planowania i zarządzania bezpieczeństwem, które są liczne i zróżnicowane, tylko metodologia DHS / FEMA prawdopodobnie zostanie ogólnie zaakceptowana. Procedury są już dobrze znane, jednolite i kompleksowe oraz uwzględniają wszystkie możliwości zagrożeń i wszystkie zasoby reagowania. Jest mało prawdopodobne, aby adwokat powoda kiedykolwiek twierdził, że działania te są niewystarczające, lub kiedykolwiek wniesie sprawę, gdy okaże się, że organizacja jest zgodna. Nie ma to na celu zniesienia wszelkiej odpowiedzialności, a jedynie ograniczenie zakresu do sytuacji zwykle objętych ubezpieczeniem.

Definicje i terminy.

Bezpieczeństwo infrastruktury informatycznej jest po prostu środkiem zapewniania wydajności SI. Dobre bezpieczeństwo wyklucza wszelkie zakłócenia IS, które mogłyby w jakikolwiek sposób obniżyć wydajność. Każde spowolnienie lub utrata wydajności, utrata danych, naruszenie prywatności lub zakłócenie systemów, sieci i narzędzi obsługujących dowolny system informacyjny zmniejsza wydajność. Dobre bezpieczeństwo zapewnia, że wszystkie systemy pozostają w pełni operacyjne, niezawodne i dokładne, a wszystkie ich dane pozostają prywatne i nie można ich narażać na szwank. Istnieją trzy elementy bezpieczeństwa systemów informatycznych. Każdy element musi być specjalnie zaprojektowany i utrzymywany w celu ochrony przed różnymi zagrożeniami o różnym zakresie i natężeniu. Te trzy elementy obejmują:

1. Bezpieczeństwo logiczne, znane również jako bezpieczeństwo systemów informatycznych, chroni jedynie integralność danych i przetwarzania informacji.

2. Bezpieczeństwo fizyczne, zwane także bezpieczeństwem infrastruktury, chroni resztę systemów informatycznych oraz wszystkich osób, które używają, obsługują i konserwują systemy. Zabezpieczenia fizyczne muszą również zapobiegać wszelkim fizycznym dostępom lub włamaniom, które mogłyby zagrozić bezpieczeństwu logicznemu.

3. Ochrona lokalu, znana również jako ochrona korporacyjna lub ochrona obiektu, chroni ludzi i mienie w całym obszarze, obiekcie lub budynku (budynkach) i jest zwykle wymagana przez kodeksy, przepisy i zobowiązania powiernicze. Bezpieczeństwo lokalu chroni szerokie obszary. Często zapewnia ochronę obwodową, kontrolę dostępu, wykrywanie dymu i ognia, tłumienie ognia, ochronę środowiska, a

zwykle systemy nadzoru, alarmy, strażników i strażników. Bezpieczeństwo lokali jest często rozszerzeniem organów ścigania.

Oczywiste jest, że każdy element nakłada się na siebie, a zagrożenie dla jednego jest często również zagrożeniem dla innych. Jednak każdy element może postrzegać i traktować każde zagrożenie inaczej. Chociaż pozostała część tego rozdziału dotyczy bezpieczeństwa fizycznego, niektóre zagrożenia, które zwykle są uważane za dziedzinę bezpieczeństwa logicznego lub bezpieczeństwa obiektów, również muszą zostać uwzględnione.

Jednolity, kompleksowy proces planowania.

Proces oceny zagrożenia może przebiegać pod wieloma nazwami, które są funkcjonalnie podobne. Są to między innymi sytuacje awaryjne, katastrofy, operacje, planowanie awaryjne i reagowania kryzysowego oraz kontrola szkód. Niektóre procesy są zastrzeżone i nie mają wspólnego języka ani standardowych procedur, które są zrozumiałe dla wszystkich zainteresowanych. Wiele regulowanych branż musi opracować plany reagowania na sytuacje kryzysowe przy użyciu warunków i formatów podyktowanych przez organ regulacyjny, co czyni te warunki i formaty zastrzeżonymi także. Istnieje wiele różnych przykładów regulowanych branż, które wykorzystują materiały niebezpieczne lub jądrowe lub obsługują zapory. Wiele organizacji zaangażowanych w reagowanie w nagłych wypadkach - takie jak szpitale i pogotowie ratunkowe, szkoły, amerykański Czerwony Krzyż i wiele agencji wolontariackich, Gwardii Narodowej i jednostek wojskowych - może nadal używać innych terminów i modeli. Agencje rządowe na poziomie lokalnym, stanowym i federalnym nadal stosują szeroką gamę planów i procedur bezpieczeństwa, mimo że obecnie wymagana jest jedna standardowa metodologia. Większość tych procedur nie jest jednolita ani kompleksowa. Mogą być niekompatybilne, stanowić główne bariery komunikacyjne i powodować niepotrzebne nieporozumienia, opóźnienia i marnowane zasoby. Z kolei większość organizacji prywatnych nie jest świadoma obowiązujących procedur rządowych ani wielu zasobów, które mogą im pomóc. Każda organizacja doświadcza zasadniczo tych samych zagrożeń i ma ograniczone możliwości reagowania i zasoby. Prawie każda organizacja może zostać przytłoczona w poważnej sytuacji kryzysowej i każdy może ogromnie skorzystać z zasobów zewnętrznych. Jednak każde miejsce ma tendencję do używania odmiennych modeli, terminów i procedur, które często są niezrozumiałe dla innych. W wielu przypadkach ich modele stają się planami i procedurami przechowywania i zapominania, których nikt nie rozumie ani nie akceptuje. Jeśli tylko jako ostrożna strategia zarządzania ryzykiem w celu uniknięcia problemów związanych z odpowiedzialnością, potrzebny jest jeden, jednolity i kompleksowy standard dla procesów, procedur i języka. Najlepszym sposobem na to jest przyjęcie metodologii DHS / FEMA, która obejmuje wszystkie zagrożenia, skutecznie koordynuje wszystkie zasoby i jest jasna, zwięzła, zrozumiała i zaakceptowana przez wszystkich zaangażowanych. Jest to teraz wymagane dla wszystkich departamentów i agencji rządowych, a także dla jurysdykcji stanowych i lokalnych, jeśli chcą one nadal otrzymywać federalne granty i pomoc. Przydatny publiczny / prywatny standard oceny gotowości na wypadek katastrofy / zagrożenia został opublikowany przez Emergency Management Assessment Program5 (EMAP), który jest niedochodową organizacją zawodową. Standard EMAP obejmuje całą aktualną metodologię DHS / FEMA i zapewnia jasną i zwięzłą metodę do ustalenia zgodności, a także proces samokontroli. EMAP zapewnia również niezależny, zewnętrzny audyt bezpieczeństwa dowolnej organizacji rządowej w celu upewnienia się, że jego program zarządzania kryzysowego jest zgodny z wymogami federalnymi; wkrótce może być w stanie przeprowadzić audyt także w prywatnych organizacjach. Audyt przeprowadzany jest w placówce wnioskodawcy przez profesjonalnych, dobrze wyszkolonych wolontariuszy. Cały proces audytu bezpieczeństwa jest zarówno rygorystyczny, jak i niedrogi. EMAP jest zatem sugerowaną alternatywą dla audytu bezpieczeństwa zapewnianego przez CPA, a także dla procedur audytu innych organizacji zawodowych, które zasadniczo nie obejmują ani bezpieczeństwa

infrastruktury, ani zgodności z procedurami federalnymi. Gotowość do zapewnienia bezpieczeństwa zgodna z tymi standardami może stać się niezbędnym warunkiem uzyskania przez sektor prywatny ubezpieczenia, uniknięcia odpowiedzialności i nadmiernych kosztów, ustalenia niewinności lub wykorzystania rynków kapitałowych do zarządzania ryzykiem. Znajomość tych standardów pomoże w procesie oceny zagrożeń, a później może zapewnić lepszą ochronę.

PROCES OCENY ZAGROŻEŃ.

Skuteczne planowanie bezpieczeństwa rozpoczyna się od dokładnej oceny zagrożenia. Proces ten rozpoczyna się od ustanowienia organizacji ad hoc, uzyskania zatwierdzenia budżetu i sponsorowania wyższej kadry kierowniczej oraz powołania komitetu sterującego, który reprezentuje wszystkie zainteresowane strony. Pierwsze cztery zadania to:

1. Zidentyfikuj wszystkie potencjalne sytuacje zagrożenia.

2. Określ prawdopodobieństwo i oszacuj bezpośrednie i pośrednie koszty każdego zagrożenia.

3. Oceń i ustal priorytetyzację każdego zagrożenia.

4. Przygotuj i przedstaw końcowe sprawozdanie, które podpisuje każdy członek komitetu.

Ten raport staje się dowodem należytej staranności w celu uniknięcia odpowiedzialności i staje się podstawą do ochrony infrastruktury. Aby nie przejść przez proces planowania, kilka osób decyduje o zagrożeniach i ryzyku, a następnie pisze plan bezpieczeństwa. Jest to odwrotne podejście do dobrego i skutecznego planowania. I to nie zadziała. Bardzo niewielu kluczowych pracowników zaakceptuje plan, a nawet go zrozumie, i prawdopodobnie zostanie zignorowany lub przeoczony, gdy pojawi się kolejny wypadek. Dobrym przykładem nieudanego planowania są plany zarządzania kryzysowego dla obszarów Nowego Orleanu i Baton Rouge, które zostały wdrożone przed Huraganem Katrina w 2005 r. najwyraźniej oba były dobrymi planami. Ale niewielu urzędników rozumiało plany lub nie pamiętało o ich wykorzystaniu. Proces planowania oceny zagrożenia musi być wykonany dokładnie i całkowicie.

Załóż komitet sterujący.

Proces planowania bezpieczeństwa nie jest skuteczny, chyba że wszyscy interesariusze są reprezentowani, a najlepszym sposobem na to jest ustanowienie komitetu sterującego. Komitet pomoże zidentyfikować i ocenić potencjalne zagrożenia oraz pomoże opracować kompleksowy plan ochrony. Komitet powinien reprezentować wszystkie zainteresowane strony i obejmować jak najwięcej doświadczenia, wiedzy i perspektywy. Interesariusze powinni obejmować użytkowników, administratorów, kierownictwo, kluczowych partnerów, klientów, dostawców i usługodawców (takich jak personel zajmujący się konserwacją, naprawą i czyszczeniem). Kierownik projektu powinien uczestniczyć, podobnie jak przedstawiciele prawni, finansowi i kadrowi. Zalecani są również niezależni eksperci i facylitatorzy. Najlepszym przewodniczącym komitetu jest zwykle zewnętrzny facylitator, który jest odporny na polityczne lub kulturowe uprzedzenia, lojalność lub preferencje dotyczące produktów. Mądrze jest także zwracać się o informacje do akcjonariuszy, pożyczkodawców, ubezpieczycieli oraz przedstawicieli społeczności i rządów. Może to być wirtualny komitet, który rzadko musi się spotykać podczas pełnej sesji. Komunikacja za pośrednictwem poczty elektronicznej lub telefonu powinna być wystarczająca, a wewnętrzny personel może gromadzić dane, wydawać raporty i współpracować z poszczególnymi członkami komitetu. Poufność nie jest w tym momencie problemem. Celem komitetu jest identyfikacja zagrożeń i pomoc w planowaniu. Żaden członek nie musi mieć pełnej wiedzy na temat rzeczywistych luk w zabezpieczeniach lub wynikających z nich systemów bezpieczeństwa i zabezpieczeń. Każdy członek powinien jednak podpisać się na raporcie końcowym komisji. Po zakończeniu początkowej misji najlepiej jest, aby komitet zbierał się co najmniej

raz w roku w celu przeglądu nowych zmieniających się zagrożeń i oceny zachowania systemów bezpieczeństwa. Komitet ten nie tylko reprezentuje wszystkie zainteresowane strony, ale może zapewnić nadzór, aby kierownictwo nie zaniedbało wykonywania, przeglądu, i zaktualizuj plan bezpieczeństwa. W rezultacie komitet dokłada należytej staranności, aby kierownictwo wypełniło swoje obowiązki powiernicze.

Zidentyfikuj wszystkie możliwe zagrożenia.

Pierwszym krokiem jest zidentyfikowanie wszystkich możliwych sytuacji zagrożenia, które mogą wpłynąć na infrastrukturę informacyjną. Nie oznacza to, że któregoś dnia zdarzy się każde zagrożenie, ale możliwe, że może to nastąpić w pobliżu lub nawet na odległość. Związek przyczynowy może być co najwyżej niepewny, a wydarzenie najbardziej mało prawdopodobne, ale może się kiedyś zdarzyć. O wiele lepiej jest myśleć obiektywnie o takich rzeczach i skutecznie planować, niż po prostu spisywać je jako zdarzenia, które mogą „nigdy się tu nie wydarzyć" lub twierdzić, że jeśli taka katastrofa się tutaj zdarzy, „nic nie możemy zrobić, aby złagodzić to. " Oba stwierdzenia są oczywiście fałszywe i potencjalnie bardzo kosztowne. Lista zagrożeń może być bardzo długa. Format powinien zawierać tabelę dla każdego konkretnego zagrożenia wraz z opisem w jednym wierszu, aby wyjaśnić, co to znaczy. Na przykład „powódź" to zbyt ogólny termin, aby w sposób znaczący ocenić ryzyko. Zamiast tego można wymienić „powodzie rzeczne", które mogą być skutkiem ulewnych deszczy, topniejącego śniegu lub pękniętej tamy lub grobli; „Lokalne powodzie", takie jak przerwa w wodzie, główna burza lub poważny pożar w pobliżu; lub „zalanie pomieszczeń", być może z powodu nieszczelnych rur, drenów lub nieszczelnych okien, dachów, niepowodzeń budowlanych, pękającego zbiornika na wodę lub chłodni kominowej lub tłumienia ognia. Celem jest stworzenie długiej listy konkretnych sytuacji zagrożenia, które można indywidualnie ocenić. Na liście może znajdować się 100 lub więcej zagrożeń. W miarę postępu projektu zaangażowane osoby z pewnością dodadzą jeszcze więcej zagrożeń i dopracowują definicje. Lista zagrożeń powinna obejmować zagrożenia zarówno bezpośrednie, jak i pośrednie oraz zagrożenia wpływające na obszar ogólny, region lub cały kraj. Najlepiej jest wymienić wszystkie zagrożenia, w tym te, które uważa się za mało prawdopodobne, jako środek ostrożności przed przypadkowym pominięciem niektórych, które mogą mieć większe znaczenie, niż jest to widoczne na pierwszy rzut oka. Niestety, zagrożenia mają tendencję do kaskadowania: jedna sytuacja zagrożenia może stworzyć inne, a te z kolei mogą stworzyć więcej sytuacji zagrożenia. Na przykład poważne powodzie mogą zamykać jezdnie i powstrzymywać ludzi od pracy, utrudniać dostawę materiałów niezbędnych do działania (takich jak żywność, woda lub paliwo do generatora awaryjnego), zakłócać komunikację, powodować zsuwanie się błota, zapalać pożary, uruchamiać grabieże lub powodować niepokoje społeczne. Jako inny przykład, podczas pożaru prawdopodobnie nastąpi utrata energii elektrycznej do chłodzenia sprzętu, wentylacji lub komunikacji, a także uwolniona woda lub chemikalia, które muszą być zawarte. Każdy z tych warunków stanowi osobne zagrożenie z własnym ryzykiem. W rzeczywistości niewiele zagrożeń występuje w oderwaniu, a wiele zdarzeń kaskadowych może być nieoczekiwanych i nieprzewidywalnych, a same mogą wywołać jeszcze więcej zdarzeń. W związku z tym zestawienie każdego zagrożenia powinno również obejmować dwie inne kolumny: (1) zdarzenia, które mogą wywołać zagrożenie, oraz (2) kaskadowe zagrożenia, które mogą wynikać z zagrożenia. Można to łatwo zrobić, numerując każde zagrożenie i wskazując numery, które mogą łączyć różne zagrożenia. Informacje są potrzebne do oceny wpływu każdego zagrożenia. Może to być jedynie ogólne wskazanie do celów planowania tego, co może się zdarzyć. Faktyczna kaskada prawdopodobnie będzie inna, ale analiza zagrożeń będzie nadal aktualna. Nie polegaj na działaniu siły wyższej - na przykład poważnego trzęsienia ziemi - jako wymówki, że dane zagrożenie może być nieuniknione. Siła wyższa nie ogranicza odpowiedzialności, ponieważ takich zdarzeń można się spodziewać i podjąć pewne kroki w celu zminimalizowania obrażeń i szkód. Z tych samych powodów akty wojenne nie mogą też usprawiedliwiać się. Wreszcie, lista zagrożeń powinna być podzielona na główne kategorie, takie

jak zdarzenia naturalne, zdarzenia wywołane przez człowieka, wandalizm, ataki, awarie systemu wsparcia i tak dalej.

Źródła informacji i pomocy.

Następnym krokiem jest kompilacja przeszłych wydarzeń: zapisy historyczne i szczegóły dotyczące tego, co się wydarzyło, kiedy i jak, jakie obrażenia i szkody wynikły, czy było ostrzeżenie, jak szybki był początek? Kompilacja powinna obejmować zdarzenia zarówno w bliskich, jak i odległych obszarach, które mogą potencjalnie powodować szkody i zakłócenia, bezpośrednio lub pośrednio. Być może bombardowania metra i autobusów w 2005 r. W Londynie lub wcześniejsze bomby w pociągach podmiejskich w Madrycie mogą mieć wpływ na amerykańskich pracowników, którzy dojeżdżają do pracy i martwią się o własne bezpieczeństwo. W miarę powiększania się listy zagrożeń, wszyscy zaangażowani muszą myśleć nieszablonowo i szukać scenariuszy, które sugerują, że w przeszłości mogą się zdarzyć. Takie myślenie może być produktywne, gdy obiektywnie bada możliwe scenariusze. Konsultant ds. Bezpieczeństwa w Nowym Jorku, współpracował z najemcami w World Trade Center i próbował zasugerować planowanie katastrof, ale został odrzucony przez właściciela, który zapewnił wszystkich, że to „najbezpieczniejsze miejsce na ziemi". Źródła informacji do zbadania obejmują biuro pogodowe, biblioteki, lokalne jednostki straży pożarnej i policji, urzędników stanowych i powiatowych, przedsiębiorstwa użyteczności publicznej, akta prasowe oraz lokalną wiedzę o przeszłych wydarzeniach w regionie. Przedsiębiorstwa energetyczne i komunikacyjne mogą dostarczać raporty o awariach, ale ich terminologia musi być zrozumiała. Na przykład „awaria elektryczna" może obejmować jedynie przerwy trwające dłużej niż pięć minut. Regionalne i stanowe organy regulacyjne, komisje użyteczności publicznej, organizacje branżowe i zawodowe oraz grupy rozwoju biznesu mogą również udzielać przydatnych informacji, gdy ich perspektywa i terminologia zostaną wyjaśnione. Wszystkie lokalne, regionalne i stanowe agencje zarządzania kryzysowego powinny teraz mieć plan ograniczania wszystkich zagrożeń, w którym wyszczególniono wszystkie zagrożenia, które wystąpiły w całej ich jurysdykcji. W ich planie powinny również znajdować się daty, opisy i lokalizacje map; informacje te mogą sięgać historycznie od stulecia lub dłużej. Każda agencja powinna mieć lokalny plan działań awaryjnych, w którym wymienione są wszystkie potencjalne sytuacje zagrożenia w obrębie ich jurysdykcji. Zwróć szczególną uwagę na dodatki i załączniki omawiające poszczególne rodzaje zagrożeń. Oprócz tego, co jest w ich planach, każda agencja powinna udzielić znacznej pomocy w opisie możliwych poważnych zagrożeń, które są spowodowane przez człowieka, wiążą się z niebezpiecznymi materiałami lub stanowią poważne zagrożenie dla zdrowia. Zagrożenia, które identyfikują, są prawdopodobnie również Twoimi zagrożeniami. Ponadto współpracuj z każdym zainteresowanym podmiotem, aby uzyskać porady na temat zagrożeń, o których wiedzą lub postrzegają. Poproś każdą osobę, aby skontaktowała się z klientami, dostawcami i dostawcami, usługodawcami, sąsiadami biznesowymi oraz konsultantami i pracownikami naukowymi. Z tych źródeł będzie wiele wiedzy specjalistycznej, perspektywy i dobrych rad. Czas szukanie go będzie dobrze spędzony. Chociaż niektóre procedury są nieaktualne, nadal istnieje wiele przydatnych danych źródłowych.

Określ prawdopodobieństwo każdego zagrożenia.

Komitet sterujący powinien rozważyć prawdopodobieństwo wystąpienia każdego zagrożenia. Najlepszym sposobem oszacowania prawdopodobieństwa jest roczne prawdopodobieństwo w skali względnej (na przykład) od 0 (brak) do 5 (bardzo prawdopodobne). Postrzegane prawdopodobieństwo raz na 100 lat (co równa się 1-procentowemu rocznemu prawdopodobieństwu) można oszacować na 1. 5-procentowe prawdopodobieństwo roczne można oszacować na 2, podczas gdy roczne prawdopodobieństwo wynoszące 20 procent lub więcej najlepiej byłoby ocenić na 5 Zagrożenia związane z niesprzyjającymi warunkami pogodowymi należy oceniać wyżej niż sugerują dane historyczne, aby uwzględnić zmieniające się wzorce pogodowe na świecie. Należy również uwzględnić

zagrożenia o prawdopodobieństwie 0, ponieważ ta wartość może być później wykorzystana do wykazania względnej podatności każdego zagrożenia. Komitet sterujący może dostosować każdą ocenę, tak jak ona obraduje, aby końcowe wyniki były użyteczne i znaczące.

Przybliżone koszty oddziaływania.

Po określeniu wszystkich możliwych zagrożeń i oszacowaniu prawdopodobieństwa każdego z nich, następnym krokiem jest, aby komitet sterujący zastanowił się nad wpływem każdego zagrożenia. Wpływ uwzględnia potencjalne straty i koszty związane z każdym zagrożeniem. (Nie rozważaj w tym momencie zagrożeń kaskadowych.) Tutaj również sugerowana jest względna skala od 1 (bardzo niska) do 5 (bardzo wysoka). Ocena wpływu 0 prawdopodobnie nie ma znaczenia, ponieważ w rzeczywistości wystąpią pewne koszty reakcji i odzyskiwania. Mogą istnieć pojedyncze czynniki potrzebne do wyjaśnienia znaczenia ogólnego wpływu. Czynniki takie mogą obejmować prawdopodobieństwo obrażeń lub śmierci, kwotę szkód majątkowych, względne koszty reakcji i odzyskiwania, a zwłaszcza w przypadku osób prywatnych i organizacji, koszty utraty działalności. Parametry każdego czynnika i zakres każdej oceny można dostosowywać w trakcie planowania, tak aby wyniki były realistyczne i znaczące. Teraz celem jest pokazanie, które zagrożenia są potencjalnie najbardziej niebezpieczne lub kosztowne, jeśli wystąpią. Planowanie oceny zagrożeń najlepiej wykonać przy użyciu najgorszego scenariusza, ponieważ tak właśnie dzieje się w rzeczywistości. Nawet wtedy faktycznie poniesione koszty mogą być znacznie wyższe niż oczekiwano. Chociaż komitet sterujący ma jedynie ograniczoną wiedzę o możliwych kosztach, przy pewnej dyskusji komitet powinien osiągnąć konsensus co do tego, która ocena ma zastosowanie do każdego z wymienionych zagrożeń. Ich odkrycia zostaną później przejrzane przez innych, którzy są w stanie lepiej przewidzieć potencjalne koszty i mogą lepiej zrozumieć, że wpływ niektórych zagrożeń jest znacznie bardziej kosztowny niż innych. Koszty oddziaływania są zarówno bezpośrednie, jak i wynikowe. Bezpośrednie wydatki mogą obejmować koszty związane z lokalizacją problemów, ustabilizowaniem systemów, naprawą i instalacją infrastruktury zastępczej, ponownym uruchomieniem, przywróceniem baz danych oraz dokładnym testowaniem danych i systemów. Inne bezpośrednie koszty, które mogą wynikać z każdego zdarzenia, to utrata wydajności użytkowników systemu, nadgodziny potrzebne do odzyskania harmonogramów produkcji, tymczasowe usługi zlecone oraz tymczasowe urządzenia lub materiały i materiały potrzebne natychmiast. Dodaj do tych potencjalnych kosztów pośrednich lub następczych, takich jak jedzenie, warunki sanitarne i zakwaterowanie; utrata działalności, klientów lub udziału w rynku, spadająca cena akcji oraz koszty działań public relations w celu kontrolowania plotek i negatywnych wiadomości. Koszty będą nadal kumulować się podczas fazy reakcji, przez cały okres rekonwalescencji i być może długo po tym. Sumy mogą znacznie przekroczyć oczekiwania.

Koszty zdarzeń kaskadowych.

Opisano możliwości i prawdopodobieństwo wystąpienia zdarzeń kaskadowych. Każde wydarzenie zwiększa koszty oddziaływania, ale określenie prawdopodobieństwa kaskadowania i wysokości dodatkowego kosztu jest w najlepszym razie wykształcone. Jeśli zdarzenia przyczynowe dla każdego zagrożenia są pokazane na liście zagrożeń, a potencjalne zdarzenia kaskadowe również tam występują, należy oszacować koszty oddziaływania każdego pojedynczego zdarzenia. Kaskada może jednak unieważnić czynniki prawdopodobieństwa. Jeśli jedno zagrożenie już występuje, inne mogą być nieuchronne, niezależnie od pokazanego prawdopodobieństwa. Całkowity koszt uderzenia będzie prawdopodobnie nieco mniejszy niż suma części. Podczas wielu zdarzeń mogą występować pewne korzyści skali, ponieważ reakcja na jedno zdarzenie może zająć się innym zdarzeniem za niewielką dodatkową opłatą. Tutaj cenne staje się doświadczenie i perspektywa komitetu sterującego, specjalistów ds. Bezpieczeństwa i zarządzania. Jednak połączone koszty muszą być nadal realistyczne, inaczej analiza kosztów i wartości będzie błędna.

Determinacja

Decyzja o tym, które zagrożenia są najważniejsze, może być subiektywna i kontrowersyjna oraz oparta na niepotwierdzonych założeniach. Sugerowane tutaj podejście daje realistyczne dane ilościowe, które jasno wskażą, które zagrożenia są najważniejsze i dlaczego. Indywidualne opinie będą się znacznie różnić. Raporty komitetu sterującego mogą dawać przybliżenia, które są statystycznie poprawne - jeśli zasady są przestrzegane i wszystko odbywa się ostrożnie. Obrady komitetu powinny zostać przejrzane przez ekspertów i kierownictwo wyższego szczebla, z wykorzystaniem obliczeń. Inną popularną alternatywą jest matryca pokazująca prawdopodobieństwo w pionie i wpływ w poziomie, oceniająca oba czynniki jako wysokie, średnie lub niskie. Daje to dziewięć poziomów podatności na każde zagrożenie, od wysokiego do wysokiego do niskiego. Taki układ nie jest ani użyteczny, ani realistyczny. Ponieważ należy uwzględnić te czynniki wpływu, które są potencjalnie bardziej kosztowne niż inne.

Gdy wszyscy ustalą prawdopodobieństwo i wpływ każdego zagrożenia, można obliczyć bieżącą podatność każdego zagrożenia. Zasadniczo podatność na zagrożenia to obliczenie łączące prawdopodobieństwo zdarzenia z tym, ile szkód może spowodować. Sugerowana metoda daje sześć poziomów podatności, od 0 (brak) do 5 (bardzo wysoka). Następne dwa kroki są nadmiernie uproszczone, ale można je dostosować do większości potrzeb. Po prostu pomnożenie czasów prawdopodobieństwa wpływu da wartości podatności od 0 do 25, co nie odzwierciedla względnych kosztów oddziaływania większości zagrożeń. Podobnie jak proste modele, jak sugerują niektóre modele.

1. Najlepiej jest zastosować kilka czynników kosztu oddziaływania, jak opisano wcześniej, a następnie połączyć każdy czynnik, stosując stałe mnożniki dla każdego z nich, aby zachować względną ważność każdego kosztu wpływu. Połączenie przez uśrednienie każdego czynnika kosztów może nie dać użytecznych wyników. Łączenie średniej wartości każdego czynnika (lub czasami najwyższa wartość) może dać bardziej realistyczne dane.

2. Na koniec przekonwertuj obliczenia podatności na skalę względną od 0 do 5 punktów, wybierając zakres wyników dla każdej wartości skali.

Wykonanie tej procedury dla wszystkich zagrożeń pokaże, że formuły, mnożniki i zakresy wartości skali mogą wymagać niewielkiej korekty, aby uzyskać znaczące wyniki. Jak już wspomniano, proste mnożenie i / lub dodawanie lub inne formuły liniowe nie przyniosą realistycznych wyników. Ważność obliczania podatności na zagrożenia polega na tym, że można to zrobić w czasie rzeczywistym, a mnożniki można również korygować w czasie rzeczywistym, gdy zmieniają się poziomy zagrożenia. Na przykład może to znaleźć odzwierciedlenie w krajowym systemie doradczym ds. Terroryzmu (NTADS) według lokalizacji lub możliwych typów docelowych. Może również wprowadzać ostrzeżenia z lokalnej policji i źródeł wywiadowczych. (Niektóre informacje o zagrożeniach są prawdopodobnie sklasyfikowane, ale dostarczony przez nie mnożnik nie jest ograniczony ani nawet wrażliwy). Wszystkie dane mogą być wyświetlane w arkuszu kalkulacyjnym, nawet do poziomu kodowania kolorami na każdym poziomie podatności. Każda osoba zaangażowana w zarządzanie bezpieczeństwem lub zarządzaniem sytuacjami kryzysowymi może mieć dostęp w czasie rzeczywistym do tych samych ekranów, które będą aktualizowane na bieżąco wraz ze zmianami warunków. Dobrze jest zapewnić wybór ekranów podsumowanych lub szczegółowo podzielonych według regionów i kategorii zagrożeń lub uszeregowanych według ważności. Wreszcie, pełne dane podatności powinny być ograniczone i dostępne tylko dla osób, które muszą to wiedzieć. Informacje te są bardzo wrażliwe; pokazuje potencjalnych przestępców tam, gdzie infrastruktura SI jest dobrze chroniona, a gdzie nie.

Wypełnianie raportu oceny zagrożenia.

Po zakończeniu szczegółowej oceny zagrożenia należy przygotować ogólny raport do przekazania wszystkim zainteresowanym stronom. Raport jest w większości tekstowy i nie sugeruje słabych punktów ani tego, czym może być ochrona bezpieczeństwa. Każdy członek komitetu sterującego powinien podpisać się w tym raporcie, podobnie jak kierownictwo wyższego szczebla i pracownicy ochrony. Celem tego raportu jest rozwinięcie świadomości bezpieczeństwa, do wykorzystania w szkoleniach oraz jako dowód należytej staranności, że rzeczywiście przeprowadzono dokładną ocenę zagrożenia.

OGÓLNE ZAGROŻENIA.

Szereg sytuacji zagrożenia może wpłynąć na infrastrukturę SI, obniżyć wydajność i wywołać niepokój, który obniży wydajność i morale. Sugerowana wcześniej lista zaczyna identyfikować niektóre z tych zagrożeń. W tej sekcji wymieniono niektóre inne możliwe sytuacje, które zasadniczo nie są związane z infrastrukturą IS. Różne zagrożenia sugerowane w tym rozdziale są jednak dalekie od pełnej listy. Dlatego należy skorzystać z porad ekspertów, lokalnej wiedzy i analizy bieżących wydarzeń, aby dostosować listę zagrożeń do konkretnych potrzeb każdej jurysdykcji, a następnie okresowo ją przeglądać i korygować. Jak wspomniano wcześniej, konkretne zagrożenia są zwykle podzielone na szerokie kategorie, które można łatwo podsumować w celu zapewnienia świadomości sytuacyjnej. Ogólnie rzecz biorąc, zagrożenia są klasyfikowane jako zagrożenia naturalne, zagrożenia techniczne i spowodowane przez człowieka, niepokoje społeczne, wandalizm i ataki. Inne mniej prawdopodobne, ale potencjalnie poważniejsze możliwości obejmują bomby, uwalnianie materiałów niebezpiecznych, pandemię i zagrożenia związane z bronią masowego rażenia. Ostateczne grupowanie może być wydarzeniami lokalnymi specyficznymi dla chronionych witryn. Same grupy nie są ważne, o ile uwzględnione są wszystkie możliwe scenariusze. Niektóre przydziały będą arbitralne, ponieważ niektóre zagrożenia można przypisać do dowolnej z kilku kategorii. (Ale nigdy nie wymieniaj żadnego konkretnego zagrożenia więcej niż raz.) Jak dotąd nie ma jednego, jednolitego, kompleksowego formatu listy zagrożeń. W miarę postępu procesu planowania najprawdopodobniej pojawią się najlepsze grupy zagrożeń.

Zagrożenia naturalne.

Zdarzenia związane z zagrożeniami naturalnymi stają się coraz częstsze, szkodliwe i rozpowszechnione, ponieważ ich wzorce wydają się zmieniać. Coraz częstsze wydarzenia obejmują poważne powodzie, silne burze; huragany i tornada; zamiecie, obfite opady śniegu i burze lodowe; pożary i gęsty dym; zanieczyszczenie powietrza, wody, budynków lub gleby; i rosnące zagrożenia chorobami. Chociaż trzęsienia ziemi zdarzają się cyklicznie, one również wydają się obecnie bardziej powszechne. Każde z nich może zakłócać działalność na wiele bezpośrednich i następczych sposobów - wiele nieprzewidzianych - w zależności od lokalizacji systemów informatycznych, sieci, terminali, przechowywania danych, kabli i mediów. Zagrożeniom naturalnym nie można zapobiec, ale ich wpływ można złagodzić. Poniżej przedstawiono dokładniejsze spojrzenie na każdą kategorię.

* Zagrożenia atmosferyczne. Mogą to być trudne warunki pogodowe, takie jak cyklony tropikalne i huragany; silne burze z huraganowymi wiatrami, silną błyskawicą i dużymi gradami; tornada; wichury; śnieżyce i ciężkie śniegi; burze lodowe; zanieczyszczenie powietrza i wysoki poziom ozonu; opad nuklearny (który zawsze występuje, ale na niskich poziomach); ekstremalnie zimno; i ekstremalnie gorąca pogoda.

* Zagrożenia geologiczne. Są to głównie osuwiska i osuwania się błota, osiadanie gruntów (doły) i gleby rozległe z powodu wody.

* Zagrożenia hydrologiczne. Zagrożenia te obejmują powodzie rzeczne i powodzie obszarów nisko położonych z powodu silnych lub długotrwałych opadów; szybki lód lub topniejący śnieg; zatory lodowe lub zanieczyszczenia na drogach wodnych; uszkodzenia wybrzeża w wyniku gwałtownego sztormu; erozja strumieni; i zawalenie się jezdni, mostów i budynków. Zdarzenia hydrologiczne mogą kaskadowo zakłócać systemy wodne i kanalizacyjne, powodować niedobory żywności i paliw, a nawet wywołać pożary lub wybuchy. Awaria tamy lub wału przeciwpowodziowego jest poważnym zagrożeniem, które należy dokładnie przeanalizować, a następnie sprawdzić z ekspertami. Większość tam jest dobrze utrzymana i chroniona przed zagrożeniami naturalnymi, ale nie przed wandalizmem ani atakiem terrorystycznym. Większość zbiorników nie jest również dobrze chroniona przed atakiem chemicznym. Konsekwencje takich wydarzeń mogą być o wiele bardziej niszczycielskie, niż się wydaje. Awaria wału przeciwpowodziowego w Nowym Orleanie w 2005 r. Spowodowana przez huragan Katrina spowodowała katastrofalne skutki na dużych obszarach. Długotrwała susza może być szczególnie destrukcyjna. Może być wiele pożarów i gęstego dymu, które wymagają ewakuacji. Brak wody pitnej i chłodzącej. Zarówno ludzie, jak i sprzęt muszą być chronione przed kurzem lub dymem, których nie można skutecznie wykonać w wielu obiektach. Energia hydroelektryczna może być racjonowana i narzucane ciągłe zaciemnienia.

* Zagrożenia sejsmiczne. Takie zagrożenia obejmują trzęsienia ziemi i tsunami. Wiele obszarów Stanów Zjednoczonych jest narażonych na umiarkowane lub nawet wysokie ryzyko dużego trzęsienia ziemi. Setki lat temu miały miejsce duże wydarzenia na tych obszarach i uważa się, że zbliża się czas ponownego wystąpienia. Na przykład uskok Ossipee w centrum New Hampshire spowodował trzęsienie ziemi o wielkości „San Francisco" około 300 lat temu i może wystąpić ponownie, co spowodowałoby znaczne szkody w Bostonie i jego przedmieściach. Przynajmniej spowodowałoby to przewrócenie szafek na sprzęt, zerwanie kabli i przewodów oraz prawdopodobnie zakłóciłoby chłodzenie i wentylację systemów IS. Tsunami, które są spowodowane przez podmorskie trzęsienia ziemi, mogą w pewnym momencie uderzyć w brzegi USA, na podstawie wydarzeń historycznych. I podobnie jak huragan Katrina, duże przedsięwzięcie sejsmiczne w dowolnym miejscu w Ameryce Północnej może mieć wpływ na firmy na dużym obszarze.

Inne zagrożenia naturalne

* Duże erupcje wulkaniczne. Erupcje wulkanów mogą rozprzestrzeniać pył atmosferyczny na całym świecie, co może wpływać na pogodę i powodować silne burze, uszkadzać systemy chłodzenia, zakłócać transmisje radiowe i satelitarne oraz ograniczać podróże lotnicze.

* Pożar. Pożar może zamknąć trasy transportu, zakłócać media i systemy wsparcia na dużym obszarze, wymagać ewakuacji i tworzyć ciężki dym, który jest niebezpieczny dla ludzi i sprzętu.

* Zaraza lub zaraza. Przyczyną choroby, pogody lub owadów, zaraza lub zaraza mogą powodować problemy zdrowotne i zakłócać dostawy żywności, co może pośrednio wpływać na działalność gospodarczą.

* Aktywność plam słonecznych. Około 11-letni cykl burz słonecznych magnetycznych, które powodują plamy słoneczne, może powodować fale promieniowania elektromagnetycznego, które mogą zakłócać komunikację, a nawet sieć elektryczną.

Zagrożenia dla zdrowia

Coraz bardziej niepokojąca jest możliwość wystąpienia nagłych problemów zdrowotnych, takich jak SARS ,COVID-19 lub wybuch wąglika lub wirus Zachodniego Nilu w stosunkowo niewielkich ilościach obszarowych. Takie ogniska mogą być prawdopodobnie powstrzymywane przez leki przeciwwirusowe

i szczepionki. Jednak z pewnością spowodują to zakłócenia w działalności gospodarczej. Bardziej niepokojące jest zagrożenie kolejną pandemią, która może szybko rozprzestrzenić się na dużych obszarach zaludnionych. Jak dotąd nie ma skutecznych środków zapobiegających ani rozprzestrzenianiu się pandemii, innych niż izolacja i kwarantanna, w tym zamykanie firm i szkół, a być może także wielu urzędów miejskich. Jak wspomniano wcześniej, jako możliwy scenariusz najgorszego przypadku, personel odmawiający lub niezdolny do zgłoszenia się do pracy podczas poważnego zagrożenia zdrowia może stanowić łącznie nawet 40 procent siły roboczej i może pozostać poza miejscem pracy nawet przez 14 miesięcy. Skonsultuj się z lokalnymi urzędnikami ds. Zdrowia, aby uzyskać szczegółowe informacje na temat tych zagrożeń.

Zagrożenia spowodowane przez człowieka.

Wypadki powodują większość problemów z bezpieczeństwem. Wypadki, niechlujstwa i błędy są konsekwencjami złego projektu, złej kontroli jakości, niewłaściwej instalacji, braku aktualizacji i złej konserwacji. Zakłócenia często występują podczas konserwacji. Rozmyślne działania, takie jak szpiegowanie, psoty, wandalizm i szpiegostwo, stają się coraz bardziej powszechne i wyrafinowane, ale wciąż pozostają w cieniu przypadkowych, niezamierzonych wydarzeń. Przenoszenie mebli lub sprzętu (chyba, że są wykonywane przez przeszkolonych specjalistów) może uszkodzić przewody, złącza i inny sprzęt w stopniu wystarczającym do awarii systemów. I choć rzadko się to zdarza, znaczne „przypadkowe" szkody mogą wystąpić podczas sporu pracowniczego lub przywiezienia na miejsce personelu niebędącego członkiem związku. Prace budowlane, przeróbki, naprawy i zmiany okablowania często powodują uszkodzenie systemów informatycznych. Załogi często układają szmatki na stacjach roboczych i sprzęcie, aby chronić przed kurzem i zanieczyszczeniami. Ale nikt nie myśli, aby najpierw wyłączyć urządzenie, więc staje się przegrzane i prawdopodobnie zawiedzie natychmiast lub wkrótce potem. Załogi podłączają również elektronarzędzia, maszyny do woskowania podłóg lub odkurzacze do dowolnych gniazdek elektrycznych, które są pod ręką. Jeśli są to dedykowane obwody dla urządzeń systemowych, może dojść do uszkodzenia. W podobny sposób użytkownicy stacji roboczych często umieszczają znaczniki czasu, zszywacze elektryczne, lodówki, wentylatory i grzałki zanurzeniowe w gniazdach przeznaczonych wyłącznie dla systemów informatycznych. Takie błędy mogą powodować sporadyczne problemy, które są trudne do zlokalizowania. Okablowanie i odsłonięty drut mogą również stanowić zagrożenie. Okablowanie jest wrażliwe na wiele sposobów - i staje się coraz bardziej. Kable danych są delikatne i łatwo ulegają uszkodzeniom w wyniku wypadku, przenoszenia mebli, czyszczenia i konserwacji, niewłaściwych połączeń (takich jak nieautoryzowany sprzęt), wściekłości lub umyślnego ataku. Druty metalowe są również wrażliwe na zakłócenia elektryczne i magnetyczne z pobliskich miejsc oprawy oświetleniowej, silniki, transformatory lub nadajniki RF, jak zostanie wyjaśnione. Błyskawica jest przyciągana i na wszelkich drutach metalowych mogą być indukowane skoki napięcia elektrycznego. Okablowanie światłowodowe, które szybko zastępuje połączenia metalowe Szybka komunikacja, jest szczególnie delikatna. Każde nietypowe ciśnienie lub ostre zagięcie dowolnego kabla światłowodowego może zmienić jego właściwości transmisyjne i spowodować awarię. Jednak na światłowód nie ma wpływu żadne wnioskowanie elektryczne ani RF. Kable, panele krosowe, kable i złącza są często narażone na przypadkowe uszkodzenie podczas rutynowej konserwacji i czyszczenia pomieszczeń. Odkurzacze oraz maszyny do mycia i woskowania mogą łatwo uszkodzić przewody sygnałowe i zasilające. Szampon do dywanów może zamoczyć połączenia i zalać przewody pod podłogą. Kółka na krzesłach i sprzęcie lub przenoszenie mebli często niszczy kable i złącza. Włamania są poważnym zagrożeniem. Istnieje wiele sposobów na uzyskanie dostępu do infrastruktury systemów informatycznych. Po udanej ingerencji mogą następować powtarzające się zakłócenia z powodu wypadków, błędów, węszenia, hakowania, szpiegowania, wandalizmu, wymuszeń lub umyślnego ataku. Kontroli dostępu do lokali zwykle nie zapobiega ingerencja. Punkty podatności infrastruktury są różne, a wczesne wykrycie jest konieczne,

aby zapobiec problemom, zanim to nastąpi. Włamania przez okablowanie zostały omówione w poprzedniej części. Nacisk kładziony jest tutaj na zapobieganie dostępowi do sprzętu, paneli dystrybucyjnych i końcowych, paneli krosowych lub dowolnych narzędzi, które je obsługują. Ocena możliwych zagrożeń polega w pierwszej kolejności na sprawdzeniu istniejącej infrastruktury i istniejących już zabezpieczeń. To jest również niezbędne do ustalenia, które fizyczne zagrożenia i punkty podatności nie są w wystarczającym stopniu objęte zabezpieczeniami lokalnymi i logicznymi.

Osobom nieupoważnionym nie należy zezwalać na dostęp do wszelkiego rodzaju urządzeń, szaf. Wszyscy, którzy uzyskali dostęp, w tym odwiedzający, powinni się zalogować i wylogować. Jako druga warstwa ochrony obszarów krytycznych strażnik powinien być pod ręką, aby obserwować każdego wchodzącego i wychodzącego, uwierzytelniać tożsamość każdej osoby i wiedzieć, dlaczego potrzebny jest dostęp. Strażnicy mogą obejmować strażników, recepcjonistów, przełożonych lub kierowników. Z wyjątkiem sytuacji, w których wymagane jest wysokie bezpieczeństwo, funkcje odszukiwania można wykonywać zdalnie za pomocą systemów nadzoru i kontroli dostępu, i monitorowane przez czujniki ruchu i zbliżeniowe. Stacje robocze znajdujące się poza pomieszczeniami sprzętowymi są na ogół chronione logicznie przy użyciu procedur logowania, tokenów, takich jak karty inteligentne i urządzenia biometryczne - w zależności od wrażliwości danych obsługiwanych przez system. Kradzież sprzętu, komponentów lub nośników wymiennych jest możliwa, szczególnie w godzinach pozabiznesowych. Zastępstwo, a nie kradzież, jest znacznie poważniejszym zagrożeniem. Jedyną bezpieczną obroną jest to, że wszystkie dane muszą być zawsze w pełni zaszyfrowane. W przypadku kradzieży jednostki zapasowe powinny być natychmiast dostępne w pobliskim bezpiecznym magazynie.

Aby zaoszczędzić czas, złodzieje często przecinają kable sygnałowe zamiast je odłączać. Dlatego mądrze jest przechowywać kable zapasowe w pobliskim bezpiecznym miejscu.Istnieją różne urządzenia zapobiegające kradzieży, służące do zaciskania lub wiązania urządzeń do pobliskich ścianek działowych lub mebli. Urządzenia te mogą być uciążliwe i uciążliwe, mogą utrudniać konserwację lub naprawy, a większość z nich szybko zostaje pokonana za pomocą nożyc do śrub lub pręta. Alarmy antywłamaniowe są bardziej skuteczne, ale wykrywają jedynie próbę włamania niż zapobiegają kradzieży. Alarmy włamaniowe są zwykle ciche i uruchamiane przy każdym otwarciu skrzynki lub szafki. Oprogramowanie może wyzwalać alarmy również wtedy, gdy kabel zostanie odłączony lub uszkodzony, lub gdy sprzęt zostanie odłączony lub ulegnie awarii. Dobry, solidny sprzęt i zamki szafek są bardziej skuteczne i mogą zniechęcać do kradzieży, pod warunkiem, że same urządzenia i szafki nie zostaną łatwo usunięte.

Podsłuchy

Podsłuchy są kolejnym sposobem włamania, którego celem jest kopiowanie danych, a czasem także ich ukradkowa zmiana. Większość podsłuchów można umieścić szybko i niepozornie, nawet w zajmowanych przestrzeniach biurowych. Większość podsłuchów jest bardzo trudna do wykrycia - jeśli nie niemożliwa - z wyjątkiem dokładnej kontroli wzrokowej wszystkich możliwych punktów wejścia, co jest czasochłonne i uciążliwe i musi być okresowo powtarzane. Bardzo często podsłuchy są po prostu niezauważane. Podsłuchy są używane do nadzoru i szpiegowania, zmiany lub usuwania danych, kradzieży oprogramowania, kradzieży usług, wstrzykiwania robaków lub wirusów lub sadzenia wabików, aby nakłonić respondentów do myślenia, że znaleźli prawdziwą przyczynę incydentu. Każdy fizyczny dostęp do punktów połączeń, przebiegów kablowych, serwerów, klientów lub sprzętu sieciowego stanowi poważną lukę. Doświadczona osoba może złożyć podsłuch w ciągu kilku minut, dyskretnie, nawet pod eskortą i uważnie obserwowana. Podsłuch jest w zasadzie urządzeniem monitorującym. Może to być niewielka skrzynka podłączona bezpośrednio do obwodu, aby odgrywać i rejestrować jego dane. Dane można następnie odzyskać ręcznie lub przesłać przewodowo lub radiowo do odległej lokalizacji, gdzie informacje mogą być trwale przechowywane i analizowane. Urządzenie monitorujące może być rozdzielaczem, który może łapać niektóre sygnały przepływające przez obwód

i przekierowywać je do usuniętej lokalizacji lub do małego nadajnika, który znajduje się w pobliżu i jest dobrze ukryty. Lepszy sprzęt do gwintowania zużywa moc systemu, a nie baterie, więc jego żywotność jest nieograniczona. Monitorowanie uzyskanych danych może odbywać się w budynku lub na zewnątrz, przez Internet, z pobliskiego pojazdu lub przez połączenie telefoniczne z dowolnym miejscem na świecie. Podsłuchy od dawna są nielegalne w Stanach Zjednoczonych bez nakazu sądowego. Lata temu, na przykład, nielegalny podsłuch telefonu w Nowym Jorku, zostało założony na dzierżawionej linii telefonicznej do Meksyku, gdzie faktyczny nadzór mógł mieć miejsce zgodnie z prawem. Połączenie zostało wykonane przez kogoś w centrali firmy telefonicznej i prawdopodobnie nie zostanie wykryte. Ale jeśli w końcu zostanie znaleziony, sieć można będzie prześledzić i odłączyć. Ta procedura sugeruje długość i koszty, do których trafi określony przeciwnik, a także sugeruje wysoką wartość informacji, które można uzyskać. To było lata temu, na długo przed dzisiejszym łatwym dostępem do Internetu, tanich połączeń międzystrefowych, Wi-Fi, mikrofalówki, satelitów i innych systemów szerokopasmowych. Obwody światłowodowe są trudne i kosztowne do dotknięcia, a czasem niemożliwe bez zerwania obwodu lub zmiany ich parametrów, co można szybko wykryć. Dostępny jest nowy sprzęt high-tech do zaczepów optycznych. Ale nawet przy tym dobre wyniki są problematyczne. Pierwsza metoda polega na utworzeniu ostrego zgięcia w kablu i wykryciu niektórych promieni świetlnych, które mogą wyciec z zewnątrz zgięcia. Sygnał jest w najlepszym razie bardzo słaby. Aby temu zapobiec, można zbudować kabel. Lub kable mogą być prowadzone przez metalowy kanał, aby uzyskać dostęp, a następnie bardzo ostre zakręt, nawet w skrzynkach przyłączeniowych. Wreszcie, ostry zakręt zmieni impedancję optyczną przebiegu kabla i nieznacznie obniży jego wydajność, być może wystarczającą do skutecznego przerwania obwodu. Zmianę impedancji optycznej można zmierzyć, w tym przybliżoną lokalizację anomalii. Metoda gięcia kabli może działać, ale jest trudna do osiągnięcia, wykrywalna i łatwa do zaobserwowania przez kontrolę. Ta metoda może monitorować dane, ale nie może wstrzykiwać danych. Jedynym bezpośrednim sposobem na podsłuch kabla światłowodowego jest otwarcie połączenia, szybkie włożenie urządzenia interfejsu, a następnie ponowne podłączenie obwodu. Alarmy powinny być uruchamiane natychmiast, gdy obwód się zepsuje lub w inny sposób ulegnie awarii, i mogą również dać pewne pojęcie, gdzie wystąpił problem. Ale z dobrym urządzeniem interfejsu i działając szybko, można wstawić podsłuch i przywrócić warunki, aby wyglądały normalnie, zanim ktokolwiek będzie mógł odpowiedzieć. Jeśli ta metoda się powiedzie, jakość przechwytywania będzie doskonała, a dane można również wstrzykiwać do linii podsłuchowej. Szpiegowanie tego, co są przenoszone przez obwody światłowodowe, może być możliwe z pomieszczeń sprzętowych lub w innych punktach, w których dane optyczne są przetwarzane na postać elektroniczną lub na fale radiowe. Sprzęt do tego i jego możliwości są ściśle tajne i na ogół nieznane większości ekspertów ds. Bezpieczeństwa. Transmisje bezprzewodowe nie muszą być podsłuchiwane, ale proces nadal obowiązuje. Wszystko, czego potrzeba, to bardzo czułe radio i antena o dużym zysku, często umieszczona w pojeździe zewnętrznym. Druty metalowe są stosunkowo łatwe do zaczepienia w niewykrywalny sposób. Małe, niepozorne cewki indukcyjne umieszczone obok drutu mogą łatwo odbierać sygnały bez penetracji izolacji. Czasami podsłuchy wykonuje się za pomocą małych sond, które sięgają obwodu drutu. Podsłuchy indukcyjne są na ogół niewykrywalne, z wyjątkiem wizualnych obserwacji. Podsłuchy indukcyjne są jednak trudne, gdy stosuje się wieloprzewodowe kable skrętkowe, zwłaszcza te, w których każda para jest ekranowana, a cały kabel jest metalowy, podobnie jak niektóre anteny telefoniczne chroniące je przed zakłóceniami o częstotliwości radiowej. Gdy indukcja nie jest praktyczna, mostkowane krany można łatwo umieścić w dostępnej puszce przyłączeniowej, panelu krzyżowym lub krosowym, skrzynce testowej lub listwie zaciskowej. Mostki kranowe mogą być połączone fizycznie. W przypadku długich kabli zwykle jedna lub więcej liniowych listew zaciskowych łączy dwa kable. Są to dobre lokalizacje dla kranów, szczególnie tam, gdzie w samym kablu mogą znajdować się nieużywane pary drutów, których można użyć do poprowadzenia danych na stukanie do bezpieczniejszej lokalizacji. Mostkowane podsłuchy można również umieszczać w dowolnym miejscu

wzdłuż drutu, penetrując izolację za pomocą igły lub odcinając niewielki kawałek okładziny i izolacji w celu splecenia drutu z kranu. Stuknięte mostki mają zwykle bardzo wysoką impedancję, więc nie zmieniają obwodu; dlatego podobnie jak kurki indukcyjne są niewykrywalne, z wyjątkiem wizualnych. Wymagana jest jednak umiejętność umieszczania ich w celu uniknięcia uszkodzenia gwintowanego przewodu. Podobnie jak w przypadku podsłuchów światłowodowych, istnieją również zaawansowane technologicznie metody monitorowania tego, co przenoszą druty metalowe, których szczegóły są klasyfikowane. Obecnie największym zagrożeniem związanym z podsłuchami jest to, że robią to zwykle obcy wywiad, przestępczość zorganizowana lub grupy terrorystyczne, które są bardzo dobrze wyposażone, dobrze wyszkolone i doświadczone oraz mają prawie nieograniczone fundusze na wykonywanie swojej pracy. Jest wysoce prawdopodobne, że większość ich nadzoru nie zostanie wykryta, zlokalizowana ani usunięta aż długo po nim - jeśli w ogóle.

Wysokoenergetyczne zagrożenia częstotliwościami radiowymi.

Kontrowersyjny obszar badań dotyczy wysokoenergetycznych broni o częstotliwości radiowej (HERF), które zdaniem niektórych ekspertów stanowią poważne zagrożenie dla zakłócenia, uszkodzenia lub zniszczenia systemów i sprzętu elektrycznego i elektronicznego na bardzo dużym obszarze. Istnieje kilka scenariuszy. Prototypowa demonstracja broni HERF na konferencjach bezpieczeństwa kilka lat temu wykazała, że nieporęczne urządzenie zbudowane z łatwo dostępnych komponentów może powodować nieprawidłowe działanie komputerów osobistych podczas działania urządzenia. Może to również powodować awarie systemu. Od tego czasu nie było już żadnych informacji publicznych, czy mniejsza, przenośna wersja mogłaby emitować wiązkę częstotliwości radiowej o mocy wystarczającej do zakłócenia działania systemów w odległości kilkudziesięciu metrów. Takie urządzenie jest możliwe, ale może nie być bardzo praktyczne, chyba że z dużego pojazdu. Wraz z tym istnieje inne zagrożenie zwane strumieniem częstotliwości radiowych o wysokiej intensywności, który jest po prostu interferencją ze strony innych urządzeń elektronicznych. Mogą to być nadajniki znajdujące się w pobliżu, takie jak radio o dużej mocy, systemy telewizyjne lub radarowe, lub nadajniki w pojazdach. Lub mogą występować zakłócenia z pobliskich nadajników RF, w tym telefonów komórkowych, komputerów i urządzeń zaprojektowanych do tego celu. Niektóre z tych możliwości to problemy projektowe, ale gdy zaangażowane są przenośne nadajniki RF, sytuacje stają się zagrożeniami dla infrastruktury. W 2004 r. zgłoszono inne podejście, które potencjalnie jest w stanie zniszczyć niezabezpieczony system elektryczny i elektroniczny w całym kraju za pomocą ataku impulsu elektromagnetycznego (EMP). Ten raport pochodzi z ustaleń komisji, że eksplozja nuklearna niskiego poziomu w górnej atmosferze może spowodować ogromną falę elektromagnetyczną, która może spowodować katastrofalne uszkodzenia w większości Stanów Zjednoczonych. Bez obszernego ekranowania systemy elektryczne i elektroniczne mogłyby zostać zniszczone, i również systemy przenoszenia mocy. Wydaje się jednak, że taka eksplozja musi zostać wykonana dokładnie tak, aby zniszczenie było minimalne. Obroną przed wszystkimi takimi zagrożeniami RF jest skuteczna ochrona sprzętu i okablowania. Klatka Faradaya może wszystko ogarnąć i chronić. Zwykle jest to jedna lub więcej warstw ekranowania miedzi, które są dobrze uziemione. Istnieją również torby Faraday do ochrony i przechowywania małych przedmiotów, takich jak telefony komórkowe lub płytki drukowane. Jednak po zainstalowaniu ekranowania dobrze jest sprawdzić, czy faktycznie działa zgodnie z oczekiwaniami. Kiedyś duże, nowe centrum danych dużego banku centrów pieniężnych., reklamując ogromne kwoty wydane na rozbudowane zabezpieczenia nowego obiektu wspomniało, że nieprzenikniona tarcza Faradaya otaczała cały pokój. Jedynym problemem było to, że radio tranzystorowe na górze szafy grało wyraźnie i głośno. Gdyby pomieszczenie rzeczywiście było dobrze ekranowane, żaden nadawany sygnał nie mógłby przeniknąć.

Incydenty z materiałami niebezpiecznymi mogą obejmować budynek, zakład przemysłowy, albo samolot, linię kolejową, autostradę lub wypadek na wodzie. Wiele niebezpiecznych substancji jest rutynowo transportowanych, przechowywanych i przetwarzanych w całych Stanach Zjednoczonych. Wiele z tych materiałów jest wyjątkowo niebezpiecznych po uwolnieniu. Mogą szybko wpłynąć na duży obszar i mogą wymagać natychmiastowej ewakuacji. Oprócz przypadkowego lub celowego uwolnienia, materiały te mogą zostać skradzione, aby stać się częścią ataku w innym miejscu. A ci, którzy próbują kraść, transportować i przetwarzać materiały na broń, mogą przypadkowo narazić innych na niebezpieczeństwo.

Toksyczne zagrożenia obejmują gromadzenie się radonu w zajmowanej przestrzeni lub w wodociągach. Radon jest uwalniany naturalnie przez wiele rodzajów skał. Jest bardzo rozpowszechniony i bardzo niebezpieczny, jeśli może dostać się do organizmu. Radon jest cząsteczką alfa, której większość tradycyjnych urządzeń pomiarowych nie może wykryć. Podobnie wiele toksycznych substancji może gromadzić się w wodzie pitnej lub powietrzu budowlanym. Każda z tych substancji będzie destrukcyjna i spowoduje niepokój daleko poza dotkniętymi obszarami. Skonsultuj się z lokalnymi urzędnikami ds. Zdrowia, aby zidentyfikować i ocenić te zagrożenia.

Ogień i dym z odległych wydarzeń mogą być kłopotliwe na kilka sposobów. Dym z wydarzeń odległych o setki mil może powodować problemy zdrowotne, opóźniać dostawy i dostawy oraz powodować niedobory żywności lub paliwa. Pracownicy mogą nie być w stanie dotrzeć do pracy lub z niej, a także mogą martwić się o swoje rodziny, przyjaciół i domy. Sprzęt elektroniczny jest szczególnie podatny na uszkodzenia środowiska spowodowane dymem lub innymi unoszącymi się w powietrzu cząsteczkami. I mogą wystąpić problemy z użytecznością lub utrata chłodzenia spowodowana dużym, odległym pożarem. Szczególnie kłopotliwy może być pożar lub dym w pobliżu. Oprócz wyżej wymienionych problemów może być konieczne natychmiastowe wyłączenie systemu i ewakuacja personelu. Linie zasilania i danych mogą być zerwane lub uszkodzone przez ciepło lub wodę.

Może również dojść do powodzi i uwolnienia niebezpiecznych materiałów, które mogą być szkodliwe dla ludzi i sprzętu. Konieczne będzie również ograniczenie zagrożeń i oczyszczenie środowiska przed wznowieniem pełnej działalności. Dym, kurz lub inne cząsteczki unoszące się w powietrzu mogą powodować awarie sprzętu, ponieważ blokują one systemy chłodzenia, zatykają filtry i gromadzą się wewnątrz urządzenia, ograniczając wentylację i chłodzenie konwekcyjne. Mimo że są to głównie problemy związane z konserwacją, stanowią one również potencjalne zagrożenia.

PRZEMOC W MIEJSCU PRACY I TERRORYZM.

Użycie siły, nękanie lub przemoc fizyczna to coraz większa rzeczywistość w miejscu pracy. Incydenty związane z narkotykami i alkoholem rosną, podobnie jak przestępstwa w miejscu pracy niezbędne do wspierania i ukrywania takich nawyków. Dodatkowym zagrożeniem jest rosnąca obecność gniewu w miejscu pracy lub na nim. Każdy z tych incydentów może powodować powszechne urazy i zakłócać działalność firmy na wiele miesięcy. Rzeczywista przemoc lub terroryzm, lub po prostu zagrożenie lub lęk przed tym, mogą być niezwykle kosztowne i destrukcyjne. Każda sytuacja przemocy - zagrożona, wyobrażona, faktyczna lub peryferyjna - może poważnie zakłócić systemy informatyczne, niezależnie od tego, czy infrastruktura jest rzeczywiście zagrożona, czy nie. Wydajność, produktywność i morale gwałtownie spadną i utrzymają się na niskim poziomie przez długi czas po zauważalnym lub faktycznym zagrożeniu. Pełne wyleczenie może potrwać wiele miesięcy - zakładając, że w międzyczasie nie zdarzy się więcej incydentów. Dlatego bezpieczne środowisko pracy, dobre planowanie i wdrażanie bezpieczeństwa oraz ćwiczenia szkoleniowe w zakresie bezpieczeństwa są niezbędne, aby wszyscy czuli się bezpiecznie.

Prawdopodobnie najlepszym narzędziem do zadawania rozległych obrażeń i szkód może być broń masowego rażenia (BMR), a nie staromodne noże, pistolety, bomby lub podpalenia, które powodują jedynie ograniczone obrażenia. Urządzenia MD są znacznie bardziej niebezpieczne, a wiele z nich jest małe i łatwe do ukrycia w kieszeni, paczce lub teczce. Mały, często wyglądający obiekt zawierający toksyny biologiczne i zasilane przez baterie latarki teoretycznie mogą zabić każdą osobę w największym budynku biurowym. Fiolka nie większa niż szminka może zawierać wystarczającą ilość wirusów hemolitycznych wirusów, aby zabić każdą osobę w promieniu od 20 do 50 km jeśli jest skutecznie zdyspergowana. Ponieważ niewiele chemicznych lub biologicznych związków BMR ma dużo zapachu lub koloru, gdy są one wypuszczane, wszyscy mieszkańcy, goście, osoby postronne i osoby reagujące mogą być niewinnymi ofiarami. Choroba może rozpocząć się w ciągu kilku minut, godzin lub dni. Analiza laboratoryjna jest konieczna do zidentyfikowania wielu substancji. Potrzeba więcej czasu, aby określić zakres i zasięg szkód. Zwykłe środki ochrony indywidualnej i aparaty oddechowe mogą zapewnić niewielką ochronę lub jej brak. BMR mogą być niezwykle niszczycielskie. Krajowe ćwiczenie szkoleniowe Departamentu Sprawiedliwości FEMA o nazwie TopOff, które przeprowadzono w maju 2000 r., symulując atak biologiczny na Denver w Kolorado, przyniosło około 57 000 ofiar śmiertelnych. Od tego czasu podobne ćwiczenia nie ujawniły oszacowań śmiertelnych. Zagrożenia BMR można pogrupować według mnemonicznego B-NICE. Obejmują one czynniki biologiczne, takie jak wąglik, cholera, dżuma płucna, tularemia, gorączka Q, ebola, ospa, botulizm, rycyna i niektóre inne. Są to wszystkie żywe bakterie, których okresy inkubacji (czas wystąpienia po ekspozycji) są mierzone w godzinach lub dniach. Uwolnienia nuklearne i radiologiczne mogą powodować panikę, ale prawdopodobnie nie spowodują masowych ofiar, z wyjątkiem osób w pobliżu. Poziomy promieniowania można łatwo monitorować, a konstrukcje budowlane często służą jako skuteczne schronienie. Urządzenia zapalające są wykorzystywane głównie do wywoływania pożarów strukturalnych. Urządzenie można sadzić w ukryciu, a następnie uruchamiać zdalnie lub za pomocą timera. Rakiety i małe pociski są coraz bardziej zapalającym zagrożeniem, podobnie jak incydenty typu 9/11: samoloty, pojazdy lub łodzie używane jako bomby. Urządzenia wybuchowe są podobne. Mogą one zostać skradzione lub przemycone zarządzeniem lub coraz częściej improwizowane urządzenia wybuchowe wykonane z powszechnie dostępnych materiałów. Możliwe są połączone ataki, takie jak urządzenia wybuchowe używane do uwalniania środków chemicznych (ale nie biologicznych, które są żywymi bakteriami, które zostałyby zabite przez wybuch) lub tak zwane brudne bomby, które są materiałami wybuchowymi używanymi do uwalniania materiałów radioaktywnych. W najgorszym przypadku wszystkie zdarzenia związane z bronią masowego rażenia mogą być wyjątkowo niebezpieczne i zakłócające, a którekolwiek z tych zdarzeń może kiedyś zdarzyć się w Stanach Zjednoczonych. Nawet plotki o AvDevent mogą być szkodliwe i powodować powszechną histerię, panikę i stworzyć dużą armię studni chodzenia. Niezależnie od tego, czy zagrożenie jest rzeczywiste, czy wymyślone, walka z bronią masowego rażenia jest kosztowna. Większość szczegółów dotyczących broni masowego rażenia oraz ekstremistycznych lub terrorystycznych zagrożeń jest niejawna, ale władze stanowe i federalne powinny być w stanie zapewnić wgląd w skuteczną ocenę zagrożenia. Należy przynajmniej zapytać władze o postrzegane zagrożenia, możliwe obszary docelowe oraz incydenty regionalne i lokalne oraz obawy dotyczące bezpieczeństwa.

INNE SYTUACJE ZAGROŻENIA

Wycieki, temperatura i wilgotność.

Należy również wziąć pod uwagę zagrożenia związane z wodą i innymi cieczami, które mogą być niebezpieczne, a także temperaturę i wilgotne warunki, w których znajduje się sprzęt. Systemy zraszaczy w pobliskich przestrzeniach mogą powodować uszkodzenie sprzętu, podobnie jak wycieki płynów ze zbiorników magazynowych, wież chłodniczych lub rur w pobliżu obszarów urządzeń.

Warunki atmosferyczne w pobliżu sprzętu to także sytuacje zagrożenia. Zbyt wysokie lub zbyt niskie temperatury powietrza mogą spowodować awarię sprzętu. Wysoka wilgotność może powodować kondensację w sprzęcie, a co gorsza, formę działania galwanicznego, które degraduje złącza, które ostatecznie ulegną awarii. Niska wilgotność jest również zagrożeniem, ponieważ sprzyja wyładowaniom elektrostatycznym, które mogą być śmiertelne dla sprzętu elektronicznego i często nie są wykrywane, dopóki sprzęt nie ulegnie awarii bez ostrzeżenia.

Odwiedzający poza godzinami pracy.

Personel zajmujący się czyszczeniem i konserwacją zwykle pracuje poza godzinami pracy i często jest zatrudniony przez wykonawcę lub właściciela, który rzadko zapewnia dużo, jeśli w ogóle, sprawdzenie przeszłości, nadzór lub szkolenie. Bardzo niewielu pracowników zdaje sobie sprawę ze środków bezpieczeństwa, a większość z nich bardzo mało wie o systemach IS, które ich praca może uszkodzić. Wielu jest źle wynagradzanych, zmuszonych jest spieszyć się z pracą i może rozumieć trochę polski. Jedno z klasycznych zakłóceń może wystąpić, gdy stacje robocze i powiązane urządzenia są po prostu podłączone do gniazdek ściennych lub przedłużaczy bez etykiet wskazujących, że nie można ich odłączać; personel sprzątający może z łatwością odłączyć takie urządzenia w sposób całkowicie niewinny, aby uruchomić własny sprzęt czyszczący, a nawet nigdy nie zauważyć, że nagle wyłączył zasilanie sprzętu komputerowego na pobliskich biurkach. Woskowanie podłóg i dywany szamponem są zwykle wykonywane poza godzinami pracy przez służby zewnętrzne. Przenoszenie mebli i zmiana stanowisk pracy są często wykonywane po godzinach, podobnie jak naprawy, zmiany w zajętej powierzchni biurowej i inne ważne czynności konserwacyjne. Prawie zawsze osoby te nie są eskortowane, a wielu z nich nie jest nawet logowanych ani wylogowanych z lokalu ani w żaden sposób zidentyfikowanych. Co gorsza, wiele z tych osób podpiera otwarte drzwi, dzięki czemu mogą pracować szybciej, a czasem mogą korzystać z klimatyzacji w sąsiednich przestrzeniach. Osoby nieznane często wchodzą do lokalu bez odpowiedniego upoważnienia. Niektórzy pracują dla właściciela lub organizacji usługowej. Niektórzy dostarczają jedzenie. Niektórzy są posłańcami. A niektórzy węszą, szpiegują, próbują ukraść, lub być może nastawieni na przemoc. Nawet pracownicy dzienni mogą pojawić się po godzinach. Dlatego najlepszą polityką bezpieczeństwa jest nie zezwalanie na nikogo po godzinach, dopóki nie zostanie pozytywnie zidentyfikowany, zalogowany i nie będzie potrzeby ustalenia. Wszystkich należy zatrzymać w recepcji lub punkcie dostawy, bez dalszego dostępu do miejsca pracy, dopóki nie zostaną odpowiednio oczyszczone. Każdy, kto wyjeżdża, również powinien zostać wylogowany, szczególnie jeśli był poza zasięgiem wzroku, gdzie wszedł. Kontrola gości w dowolnej godzinie ma dodatkową zaletę w zakresie bezpieczeństwa, ponieważ osoby z zewnątrz nie widzą, gdzie może znajdować się infrastruktura IS lub gdzie są przechowywane pieniądze, portfele lub torebki. Aby zapobiec wejściu do wrażliwego obiektu, należy użyć dzwonka nocnego lub domofonu za zamkniętymi drzwiami.

Zagrożenia związane z czyszczeniem i konserwacją.

Maszyna do woskowania podłogi niszczy wszystko, czego dotknie, i bardzo szybko niszczy niezabezpieczone okablowanie, złącza, zwisające przewody lub niewidoczne przedłużacze zasilania (które, nawiasem mówiąc, są nielegalne zgodnie z większością kodów elektrycznych). Operator maszyny do woskowania często nie widzi żadnego z tych przedmiotów lub może nie mieć czasu na dokładne przyjrzenie się temu, co jest wyraźnie widoczne. Szampon do dywanów zużywa dużo płynu i może zalać skrzynki wylotowe na poziomie podłogi i spłynąć do kanałów i kanałów podłogowych. Wtyczki elektryczne, gniazda i nieautoryzowane przedłużacze do urządzeń krytycznych są często nieznakowane. Personel sprzątający nie wie, że są krytyczni, i może nieświadomie odłączyć serwery, aby zasilić sprzęt czyszczący. Dlatego ocena zagrożenia musi najpierw ustalić, czy projekt lokalu stwarza problemy, nawet jeśli personel sprzątający i konserwujący wykonują swoją pracę ostrożnie.

Użytkownicy często wzmacniają te zagrożenia. Wiele stacji roboczych może być wylogowanych, ale nadal działają. Nikt nie każe użytkownikom wyłączać i zakrywać sprzętu przed poważnym czyszczeniem lub konserwacją.

Zagrożenia w przechowalni

Pomieszczenia używane do przechowywania materiałów komputerowych, papieru lub formularzy są szczególnie niebezpieczne w przypadku pożaru. Na przykład przechowywane kartony papieru, formularze lub artykuły papiernicze rozszerzają się, gdy się palą, a następnie wybuchają w pożarze, który szybko się rozprzestrzenia i pali w bardzo wysokiej temperaturze. Taki pożar miał miejsce w wieżowcu na Manhattanie. Mimo że straż pożarna szybko powstrzymała pożar, niektóre stalowe kolumny budynków były tak osłabione przez ciepło, że budynek prawie się zawalił. Przyczyną tego pożaru był niedopałek papierosa który wpadł między ułożone w stos kartony papieru. Zakładano, że było to przypadkowe, ale równie dobrze mogło być podpaleniem. Każde pomieszczenie zawierające wrażliwe lub łatwopalne materiały musi posiadać czujniki dymu, tryskacze lub inne zatwierdzone systemy tłumienia ognia zaprojektowane w celu ochrony zarówno pomieszczenia, jak i jego zawartości. W pobliżu muszą znajdować się również gaśnice. Pomieszczenia magazynowe powinny być zamknięte, a dostęp powinien być ograniczony do zaufanych osób, choćby w celu ochrony wartości zawartości. Powinny istnieć systemy kontroli dostępu z dopuszczeniem ograniczonym tylko do upoważnionych osób, z zapewnionymi alarmami o otwartych drzwiach. Osoby doręczające powinny zawsze być stale eskortowane. Kręcenie się, palenie, picie, narkotyki, drzemki lub wszelkie działania towarzyskie muszą być trzymane z dala od wszystkich miejsc przechowywania.

Nagłe wypadki medyczne.

Większość nagłych przypadków medycznych spowoduje zakłócenia w działalności gospodarczej. Ludzie przestają pracować, aby zobaczyć, co się dzieje, a jeśli znają ofiarę, mogą pozostać zdemoralizowani i nieproduktywni przez kolejne tygodnie. Wielu skupia się na okolicznościach i coraz częściej angażuje innych, by pogłębić problemy. Nawet niewielkie nagłe wypadki medyczne mogą powodować duże i długie zakłócenia. W wielu sytuacjach medycznych pierwsze pięć minut może zadecydować o życiu lub śmierci, a profesjonalna pomoc medyczna prawdopodobnie nie jest tak szybko niedostępna. Każda śmierć, która nastąpi w miejscu pracy, spowoduje długoterminową, powszechną i trwałą traumę i zakłócenia. W każdym miejscu pracy muszą znajdować się środki pierwszej pomocy, tlen i automatyczne defibrylatory elektryczne (AED). W pobliżu muszą znajdować się osoby przeszkolone i certyfikowane w zakresie resuscytacji sercowo-naczyniowej i pierwszej pomocy. Same koszty zakłóceń są znacznie wyższe niż koszty zapewnienia wystarczającej ilości sprzętu medycznego, sprzętu i szkolenia. Ponadto pokój pierwszej pomocy i przeszkolona pielęgniarka to mądre środki ostrożności i prawdopodobnie również oszczędności. Szybka pomoc medyczna jest niezbędna dla wyższej kadry kierowniczej, odwiedzających oraz wszystkich pracowników i gości. Zagrożenia medyczne pojawią się i będą bardzo kosztowne, jeśli pomoc medyczna nie będzie natychmiast dostępna.

Nielegalna stacja robocza.

Wygodną metodą skonfigurowania logicznego włamania lub ataku jest odłączenie terminala stacjonarnego lub stacji roboczej o ograniczonej funkcjonalności i zastąpienie w pełni funkcjonalnej maszyny dobrze zaprogramowanej programami szpiegującymi i narzędziami analitycznymi. Każdy, kto ma w pełni funkcjonalny komputer przenośny i fizyczny dostęp do sieci, może łatwo się połączyć. Nielegalni użytkownicy mogą wtedy być w stanie zalogować się do sieci, prawdopodobnie wprowadzając własne zaufane hasło użytkownika. Mogli następnie wyszukiwać ograniczone informacje i używać w pełni funkcjonalnego urządzenia do kopiowania danych sieciowych. Następnie nielegalny użytkownik po prostu łączy się z pobliskim gniazdkiem telefonicznym, aby eksportować dane

sieciowe za pośrednictwem połączenia telefonicznego. (Zapora prawdopodobnie zablokuje połączenie internetowe). Nielegalny użytkownik może użyć programów hakerskich, aby uzyskać status nadzorcy, a oprogramowanie szpiegujące może uzyskać dostęp do bardziej wrażliwych informacji, złamać hasła, ukraść oprogramowanie lub zainfekować sieć złośliwym oprogramowaniem. Nielegalny użytkownik może zainstalować wejście backdoor do sieci, którego wspólnik może używać do szpiegowania, monitorowania ruchu sieciowego oraz modyfikowania lub niszczenia danych. Doświadczony użytkownik może następnie usunąć wszystkie dowody włamania. Włamania może dokonać wewnętrzny pracownik, kontrahent, technik serwisowy, sprzedawca lub konsultant, który mógłby naruszyć sieć podczas rzekomego sprawdzania komputera użytkownika lub połączenia LAN. Można to również zrobić w strefie gorącej przy użyciu połączenia Wi-Fi, w którym może istnieć niewiele zapory ogniowej lub zabezpieczeń. Personel serwisowy pracujący poza godzinami pracy może również niepozornie zastąpić terminal. Niezależnie od tego, włamanie jest poważnym zagrożeniem fizycznym. Świadomość bezpieczeństwa to najlepsze zapobieganie. Nikt nie powinien wymieniać urządzeń ani połączeń, chyba że kierownik, przełożony lub pracownicy w pobliżu znają tożsamość osoby i jej działania. W przypadku jakichkolwiek wątpliwości należy zgłosić aktywność. Drugim najlepszym sposobem zapobiegania jest dobre bezpieczeństwo sieci z alarmami, gdy którykolwiek system pulpitu zostanie otwarty, odłączony lub zamknięty.

Inne lokalne zagrożenia.

Istnieje wiele sytuacji zagrożenia specyficznych dla grupy, organizacji lub społeczności. Zazwyczaj wiele z tych sytuacji jest identyfikowanych i ocenianych w miarę postępu planowania. Na przykład dla społeczności ważne lokalne zagrożenia mogą obejmować wandalizm lub faktyczne uszkodzenie budynków szkolnych, placów szkolnych lub autobusów szkolnych, zawalenie się budynku lub mostu, przerwane systemy transmisji energii lub energii, uszkodzone magazyny paliwa lub awarię komunikacji. Wiele możliwych konkretnych sytuacji zostanie prawdopodobnie omówionych podczas procesu planowania, a przegląd i porady ekspertów zewnętrznych i urzędników państwowych prawdopodobnie doprowadzą do ważniejszych sytuacji. Niektóre uwagi dotyczące lokalnych zagrożeń:

* Zakłócenia narzędzi. Zakłócenia zdarzają się częściej niż zgłaszane. Przerwy w dostawie prądu mogą trwać kilka minut, godzin lub dni, spowodowane uszkodzeniem przez burzę, awarią sprzętu, gałęziami drzew uderzającymi w linie energetyczne, wypadkami na autostradzie, które obalają słupy, kopaniem wypadków, które zrywają linie przesyłowe, oraz wandalizmem lub gorzej, np. wieże liniowe. Coraz częściej pojawiają się doniesienia o wieżach transmisyjnych i słupach użytkowych umyślnie przewróconych, awariach zasilania spowodowanych rozbiciem izolatorów lub przecięciu drutów pociskami, a także o awariach, które miały miejsce, gdy ukradziono przewody i szyny zbiorcze za wartość metalu w nich zawartego. W dowolnym momencie mogą występować zakłócenia statyczne lub radiowe lub skoki na linii elektroenergetycznej z powodu warunków atmosferycznych, wyładowań atmosferycznych lub przełączania urządzeń zasilających. Przerwy w komunikacji mogą być jeszcze bardziej problematyczne i niewiele z tych sytuacji są powszechnie znane. Dostawcy usług komunikacyjnych są przedsiębiorstwami nastawionymi na zysk i nie mogą zapewnić dużej ochrony przed awarią, tworzenia kopii zapasowych lub redundancji, gdy zła pogoda, wandalizm, celowe ataki lub awaria sprzętu przerywają ich usługi. Chociaż nie ma wielu alternatywnych dostawców do wyboru, jedynymi zabezpieczeniami bezpieczeństwa są redundancja i alternatywni dostawcy.

* Zakłócenia cywilne, polityczne i gospodarcze. Takie zakłócenia mogą wskazywać na podwyższony poziom zagrożenia bezpieczeństwa wewnętrznego lub alarmy stanowe lub regionalne. Inne możliwe destrukcyjne wydarzenia obejmują demonstrację, marsz, nieuporządkowaną grupę lub niesforny tłum. Inne sytuacje kryzysowe obejmują zamknięcie zakładu, strajk lub blokadę, awarię transportu lub zamknięcie. Istnieją również groźby wszelkiego rodzaju przemoc; incydent lub porwanie zakładnika;

sabotaż dowolnej infrastruktury (np. linii energetycznych); zanieczyszczenie żywności, wody, powietrza lub gleby; niedobór żywności lub paliwa, skok kosztów energii lub niedobór; oraz skutki poważnej ewakuacji gdzieś w regionie.

* Skoordynowane ataki. Te ataki są również możliwe, być może nawet przez terrorystów. Tutaj atakuje się wiele punktów infrastruktury jednocześnie i można zastosować wiele form ataku. Mogą istnieć różnorodności w celu sadzenia urządzeń do inwigilacji, umieszczania silniejszej broni lub po prostu odwracania uwagi zespołów reagujących i zmniejszania ich zasobów. Niezależnie od tego, czy szpiegostwo jest zamierzone, czy nie, celem skoordynowanego ataku jest maksymalne uszkodzenie i zakłócenie.

* Burze słoneczne. Aktywność słoneczna może również powodować duże problemy. Plamy słoneczne wpływają na systemy dystrybucji energii elektrycznej, a także na systemy elektroniczne i mogą poważnie zakłócać komunikację satelitarną, mikrofalową i awaryjną oraz transmisje radiowe, telewizyjne i radarowe.

ZAGROŻENIA INFORMACJI POUFNYCH

Wiele innych scenariuszy zagrożeń nie powinno być opisanych publicznie, ponieważ są łatwe do wykonania przez każdego, kto ma pretensje i mają skłonność do podżegania naśladowców. Inne zagrożenia, które nie zostaną opisane, wykorzystują proste narzędzia lub urządzenia, które są łatwo dostępne, są niepozorne do użyci i można bezpiecznie ukryć po przestępstwie. Unikanie takich zagrożeń jest trudne, a obawy mało prawdopodobne. Niemniej jednak złagodzenie jest możliwe, a czasem nawet odstraszające, gdy zagrożenia te zostaną znane i zrozumiane. Większość dostawców, instalatorów i konsultantów ma długie listy takich niewątpliwych zagrożeń i sposobów, w jakie wiedzą, jak zakłócać, szpiegować lub niszczyć określone typy systemów informatycznych. Żadna ocena zagrożenia nie może być kompletna bez pytania wszystkich źródeł informacji o metody ataku, jakie mogą zasugerować, a także o metody zapobiegania lub łagodzenia każdego zagrożenia. Wiele użytecznych źródeł informacji i wskazówek nie jest ogólnie dostępnych publicznie - wiele źródeł, których wyszukiwarki internetowe nie odkryły. Niektóre z tych materiałów po prostu nie są publicznie dostępne, a inne źródła mogą pochodzić z dokumentów niejawnych. Jednak informacje i zredagowane informacje mogą zostać udostępnione tym, którzy ich potrzebują. Więcej informacji może być dostępnych od władz lokalnych, stanowych i federalnych, organów regulacyjnych, grup rówieśniczych, stowarzyszeń biznesowych lub dostawców, grup zawodowych oraz ekspertów i konsultantów ds. Bezpieczeństwa. Każde z tych źródeł może chcieć udostępniać informacje niedostępne dla ogółu społeczeństwa. FBI jest ostatecznym źródłem informacji o zagrożeniach. Ale te informacje są w większości tajne i bez odpowiedniego poświadczenia bezpieczeństwa i potrzeby dowiedzenia się, FBI nie ujawni wiele. Ogólnokrajowa grupa osób zaangażowanych w bezpieczeństwo IS jest sponsorowana przez FBI i zapewnia pewne przydatne (wrażliwe, ale niesklasyfikowane) informacje, po sprawdzeniu i zatwierdzeniu każdego członka. Ta grupa nazywa się InfraGard, a w większości stanów istnieją oddzdziały. Odwiedź www.infragard.net, aby uzyskać listę lokalnych rozdziałów i skontaktuj się z nimi w sprawie członkostwa.

PODSUMOWANIE.

Szeroka gama możliwych zagrożeń fizycznych może zakłócać infrastrukturę systemów informatycznych, a tym samym zakłócać produktywność i wydajność firmy. Lista konkretnych zagrożeń może identyfikować kilkaset sytuacji, a każda z nich powinna zostać uwzględniona i uwzględniona podczas procesu oceny zagrożenia . Niektóre sytuacje zagrożenia są oczywiste i dobrze znane, podczas gdy wiele innych jest mniej znanych. Wiele z nich powstaje na nowo, sugerowane przez ostatnie wydarzenia na całym świecie i przez ponowną analizę danych historycznych. Istnieją również kwestie

apatii, zaprzeczenia i ignorancji, w których niektóre osoby uważają, że takie rzeczy nigdy na nich nie wpłyną lub że nic nie można zrobić, aby zapobiec katastrofie. Oba twierdzenia są oczywiście fałszywe i potencjalnie bardzo kosztowne, jeśli zostaną zrealizowane. Większość sytuacji zagrożenia może i kiedyś nastąpi gdzieś. Ale to, czy robią to, czy nie, jest kwestią statystyki, a nie przypuszczeń.

Każdą możliwą sytuację zagrożenia można w pewnym stopniu złagodzić poprzez staranne planowanie bezpieczeństwa i odpowiednie zarządzanie w celu zminimalizowania obrażeń i szkód. W rzeczywistości dobre bezpieczeństwo fizyczne może być niedrogie, skuteczne i wydajne. Pierwszym krokiem jest dokładna ocena zagrożenia w celu zidentyfikowania i rozważenia wszystkich możliwych sytuacji zagrożenia. Następnym krokiem jest określenie prawdopodobieństwa wystąpienia każdego zagrożenia, potencjalnego wpływu, jeśli tak się stanie, oraz podatności organizacji w kontekście jej bieżących zabezpieczeń. Każdy krok można obliczyć statystycznie, aby określić najlepsze możliwe opcje. Ten rozdział rozpoczyna proces oceny zagrożenia, który uwzględnia wszystkie te czynniki. Te rozdziały opierają się na jednolitej i kompleksowej metodologii zalecanej przez rząd federalny i teraz są wymagane dla wszystkich federalnych, stanowych i lokalnych