Cyberbezpieczeństwo i duże firmy

Wiele wyzwań związanych z bezpieczeństwem informacji, przed którymi stoją duże przedsiębiorstwa i małe firmy, jest takich samych. W rzeczywistości w ciągu ostatniej dekady oferty oparte na chmurze przyniosły małym firmom wiele dobrze chronionych systemów z technologiami klasy korporacyjnej, zmniejszając niektóre historyczne różnice między firmami różnej wielkości, jeśli chodzi o architekturę niektórych systemów. . Oczywiście wiele zagrożeń bezpieczeństwa skaluje się wraz z wielkością przedsiębiorstwa, ale nie różnią się one jakościowo w zależności od liczby pracowników, partnerów i klientów, których ma firma, ani wielkości jej budżetu na technologie informacyjne. Jednocześnie jednak większe firmy często borykają się ze znacznymi dodatkowymi komplikacjami - czasami o rząd wielkości bardziej złożonymi niż wyzwania cyberbezpieczeństwa stojące przed małymi firmami. Duża liczba różnorodnych systemów, często rozmieszczonych w różnych lokalizacjach, z niestandardowym kodem itp., Często sprawia, że zabezpieczenie dużego przedsiębiorstwa jest dość trudne i złożone. Na szczęście jednak większe firmy mają zwykle znacznie większe budżety na zakup obrony i obrońców. Ponadto, pomimo faktu, że wszystkie firmy teoretycznie powinny mieć formalne programy bezpieczeństwa informacji, małe firmy zwykle tego nie robią, podczas gdy duże firmy prawie zawsze. W tym rozdziale omówiono niektóre obszary, które mają nieproporcjonalny wpływ na duże firmy.

Wykorzystanie złożoności technologicznej

Duże przedsiębiorstwa często mają wiele biur i linii biznesowych, wiele różnych systemów informatycznych, złożone ustalenia biznesowe z partnerami i dostawcami itd. - wszystko to znajduje odzwierciedlenie w znacznie bardziej skomplikowanej infrastrukturze informatycznej, niż zwykle ma to miejsce w przypadku mniejszych przedsiębiorstw. W związku z tym duże firmy mają znacznie większą powierzchnię ataku - to znaczy mają o wiele więcej potencjalnych punktów ataku niż małe firmy - a zróżnicowane systemy oznaczają, że żadna osoba, a nawet niewielka liczba osób nie może być ekspertami w rozwiązywaniu wszyscy. Duże firmy używają mieszanki systemów chmurowych i lokalnych, systemów komercyjnych gotowych do użycia i niestandardowych, mieszanki technologii, złożonych architektur sieciowych itd. - a ich zespoły ds. Bezpieczeństwa muszą upewnić się, że wszystkie te elementy działają razem w bezpieczny sposób.

Zarządzanie systemami niestandardowymi

Duże przedsiębiorstwa prawie zawsze mają dużą liczbę niestandardowych systemów technologicznych, którymi zarządza się na miejscu. W zależności od tego, w jaki sposób są wdrażane i wykorzystywane, systemy te mogą wymagać takiego samego poziomu poprawek bezpieczeństwa, jakiego wymaga standardowe oprogramowanie - co oznacza, że pracownicy wewnętrzni muszą utrzymywać kod z punktu widzenia bezpieczeństwa, wypychać łaty i tak dalej . Ponadto zespoły bezpieczeństwa muszą być zaangażowane w systemy wewnętrzne przez cały cykl życia systemu - w tym fazy takie jak wstępne badanie, analiza i definicja wymagań, projektowanie, rozwój, integracja i testowanie, akceptacja i wdrażanie, bieżące operacje i konserwacja, ocena, i utylizacja. Bezpieczeństwo jako element tworzenia oprogramowania to skomplikowana sprawa. Całe książki są napisane o zapewnianiu bezpieczeństwa w cyklu życia oprogramowania, a także w tym obszarze przyznawane są profesjonalne certyfikaty.

Planowanie ciągłości i odtwarzanie po awarii

Chociaż małe firmy powinny mieć plany ciągłości działania i odtwarzania po awarii (czasami nazywane BCP i DRP) i powinny również regularnie testować te plany, zazwyczaj mają, przynajmniej z formalnego punktu widzenia, podstawowe plany - w najlepszym razie. Duże firmy mają zazwyczaj znacznie bardziej formalne plany - w tym szczegółowe ustalenia dotyczące wznowienia pracy w przypadku

niedostępności obiektu i tak dalej. Całe książki obejmują odzyskiwanie po awarii i planowanie ciągłości - świadectwo złożoności i niezawodności odpowiednich procesów.

Patrząc na przepisy

Duże przedsiębiorstwa często podlegają znacznie więcej przepisom, prawom, wytycznym i standardom branżowym niż małe firmy. Oprócz wszystkich zagadnień opisanych w rozdziale poświęconym na przykład zabezpieczaniu małych firm, poniższe sekcje obejmują inne, które mogą mieć wpływ na duże przedsiębiorstwa.

Sarbanes Oxley

Ustawa Sarbanes Oxley z 2002 r., technicznie znana jako ustawa o reformie rachunkowości spółek publicznych i ustawie o ochronie inwestorów lub ustawa o odpowiedzialności, odpowiedzialności i przejrzystości korporacyjnej i audytorskiej, ustanowiła wiele zasad mających na celu pomoc w ochronie inwestorów w spółkach publicznych. Na przykład wiele jego zadań ma na celu poprawę dokładności, obiektywizmu i wiarygodności oświadczeń i ujawnień korporacyjnych oraz stworzenie formalnych systemów kontroli wewnętrznej i równowagi w przedsiębiorstwach. SOX, jak to często jest znane, wprowadził surowsze zasady ładu korporacyjnego, zamknął różne luki księgowe, wzmocnił ochronę sygnalistów i stworzył znaczne kary (w tym kara więzienia) za nadużycia korporacyjne i wykonawcze. Jak sama nazwa wskazuje, wszystkie amerykańskie spółki będące własnością publiczną podlegają SOX, podobnie jak spółki spoza Stanów Zjednoczonych, które zarejestrowały jakiekolwiek udziałowe lub dłużne papiery wartościowe w amerykańskiej Komisji Papierów Wartościowych i Giełd (SEC). Ponadto każda strona trzecia, taka jak firma księgowa, która świadczy usługi księgowe lub inne usługi finansowe firmom regulowanym przez SOX, jest sama upoważniona do przestrzegania SOX, niezależnie od jej lokalizacji. SOX ma wiele konsekwencji dla bezpieczeństwa informacji - zarówno bezpośrednio, jak i pośrednio. Dwie sekcje SOX skutecznie upoważniają firmy do wdrażania różnych zabezpieczeń bezpieczeństwa informacji:

* Sekcja 302 SOX dotyczy odpowiedzialności korporacyjnej za stosowanie mechanizmów kontrolnych w celu zapewnienia, że firma sporządza dokładne raporty finansowe i wymaga od firm wdrażania systemów zapobiegających wszelkim nieuprawnionym manipulacjom w danych firmowych wykorzystywanych do tworzenia takich raportów - niezależnie od tego, czy fałszowanie jest dokonywane przez pracowników, czy ludzie.

* Sekcja 404 jest prawdopodobnie najbardziej kontrowersyjną częścią SOX i na pewno, dla wielu firm, najdroższą, której należy przestrzegać. Ta sekcja nakłada na menedżerów korporacji odpowiedzialność za zapewnienie, że firma posiada adekwatne i skuteczne struktury kontroli wewnętrznej oraz wymaga, aby wszelkie istotne niedociągnięcia były zgłaszane opinii publicznej. Artykuł 404 nakłada na kierownictwo odpowiedzialność za zapewnienie, że korporacja może właściwie chronić swoje systemy przetwarzania danych i ich zawartość, a także upoważnia firmę do udostępnienia wszystkich istotnych danych audytorom, w tym informacji o wszelkich potencjalnych naruszeniach bezpieczeństwa.

Oprócz tych dwóch obszarów, w których SOX odgrywa rolę, specjaliści ds. Bezpieczeństwa informacji prawdopodobnie będą mieli do czynienia z wieloma innymi systemami, które firmy wdrożyły w celu spełnienia innych wymagań SOX. Takie systemy wymagają ochrony, podobnie jak one same muszą przestrzegać SOX. SOX jest skomplikowany, a firmy publiczne zwykle zatrudniają osoby, które są ekspertami w zakresie odpowiednich wymagań. Z takimi osobami prawdopodobnie będą się kontaktować specjaliści ds. Bezpieczeństwa informacji.

Bardziej rygorystyczne wymagania PCI

Standardy PCI DSS dotyczące ochrony informacji o kartach kredytowych obejmują bardziej rygorystyczne wymagania dla większych firm (na przykład przetwarzających więcej transakcji kartami kredytowymi) niż dla mniejszych firm. Należy również pamiętać, że z praktycznego punktu widzenia większe firmy prawdopodobnie będą miały więcej terminali przetwarzających i więcej danych dotyczących kart kredytowych, a także bardziej zróżnicowaną technologię zaangażowaną w procesy przetwarzania kart kredytowych - co podnosi stawkę, jeśli chodzi o PCI. Większe firmy są również narażone na większe ryzyko utraty reputacji: naruszenie standardów PCI DSS przez większą firmę jest o wiele bardziej prawdopodobne, że pojawi się w ogólnokrajowych wiadomościach, niż gdyby tego samego naruszenia dokonał sklep rodzinny.

Zasady udostępniania danych spółek publicznych

Spółki publiczne - to znaczy przedsiębiorstwa publiczne, których akcje są notowane na giełdzie (lub na różnych innych publicznych platformach obrotu) - podlegają licznym zasadom i regulacjom mającym na celu ochronę integralności rynków. Jednym z takich wymogów jest to, że firma musi jednocześnie udostępniać całemu światu różnego rodzaju informacje, które mogą mieć wpływ na wartość akcji spółki. Firma nie może na przykład udostępniać takich informacji bankom inwestycyjnym przed ujawnieniem ich mediom. W rzeczywistości każdemu, komu firma ujawnia informacje przed ich publicznym ujawnieniem - na przykład księgowości spółki publicznej lub kancelariom prawnym - surowo zabrania się obrotu akcjami lub jakimkolwiek instrumentem pochodnym opartym na nich na podstawie tych danych. W związku z tym duże korporacje często stosują różnego rodzaju polityki, procedury i technologie w celu ochrony wszelkich danych podlegających takim regulacjom - oraz do reagowania na sytuacje, w których niektóre takie dane zostały nieumyślnie ujawnione.

Ujawnienia dotyczące naruszeń

Niektóre zasady dotyczące ujawniania naruszeń wyłączają mniejsze firmy, ale wszystkie wymagają ujawniania informacji od dużych przedsiębiorstw. Ponadto duże przedsiębiorstwa często mają wiele działów, które muszą współdziałać i koordynować działania w celu ujawnienia informacji o naruszeniu - czasami również z udziałem stron zewnętrznych. Przedstawiciele działów marketingu, relacji inwestorskich, technologii informatycznych, bezpieczeństwa, prawny i innych, na przykład, mogą potrzebować współpracować w celu skoordynowania treści wszelkich informacji i mogą wymagać zaangażowania zewnętrznej firmy public relations i zewnętrznego doradcy, dobrze. Duże przedsiębiorstwa mają również zazwyczaj oficjalnych rzeczników i działy mediów, do których prasa może kierować wszelkie pytania.

Regulatory i przepisy branżowe

Różne przepisy i regulacje branżowe mają zwykle zastosowanie do większych firm częściej niż do małych firm. Na przykład Nuclear Regulatory Commission (NRC), która jest niezależną agencją federalną, która reguluje spółki energetyki jądrowej w Stanach Zjednoczonych, reguluje niektóre główne zakłady użyteczności publicznej, ale niewiele, jeśli w ogóle, sklepów typu „mom and pop" będzie podlegać jej przepisy prawne. Dlatego tylko większe firmy przeznaczają znaczne zasoby na zapewnienie zgodności z jej zasadami. W świecie przepisów NRC cyberbezpieczeństwo jest ważnym elementem w zarządzaniu różnymi systemami nadzoru i akwizycji danych (SCADA), które są komputerowymi systemami sterowania i zarządzania, które komunikują się z kontrolerami w komponentach zakładu. Podobnie, z wyjątkiem niektórych funduszy hedgingowych i innych operacji finansowych, niewiele małych firm jest zobowiązanych do monitorowania i rejestrowania wszystkich interakcji w mediach społecznościowych swoich pracowników, tak jak duże banki muszą to robić w przypadku niektórych pracowników. W wyniku przepisów branżowych wiele dużych firm stosuje różne

procesy, zasady i technologie, które generują dane i systemy wymagające wszelkiego rodzaju zaangażowania w bezpieczeństwo informacji.

Obowiązki powiernicze

Podczas gdy wiele małych firm nie ma zewnętrznych udziałowców, za których zarząd lub zarząd może ponosić bezpośrednią odpowiedzialność, większość dużych korporacji ma inwestorów, którzy mogą pozwać jedną lub obie strony, jeśli naruszenie cyberbezpieczeństwa zaszkodzi wartości firmy. Różne przepisy wymagają od kierownictwa i zarządów zapewnienia odpowiedniego zabezpieczenia systemów. W niektórych przypadkach ludzie mogą nawet zostać oskarżeni o popełnienie przestępstwa, jeśli dopuścili się zaniedbania. Nawet jeśli menedżerowie wyższego szczebla nie zostaną oskarżeni po naruszeniu, nadal mogą ponieść poważne szkody w karierze i reputacji z powodu niepowodzenia w zapobieganiu temu.

Głębokie kieszenie

Ponieważ duże przedsiębiorstwa mają znacznie głębsze kieszenie niż małe firmy - innymi słowy, mają do dyspozycji znacznie więcej pieniędzy - i ponieważ kierowanie reklam na sklepy dla mam i popów nie jest zwykle tak korzystne politycznie, jak kierowanie reklam do dużej firmy, która wykazała się złymi zachowania, organy regulacyjne mają tendencję do prowadzenia spraw dotyczących zgodności z dużymi przedsiębiorstwami podejrzanymi o naruszenia ze znacznie większym zapałem niż wobec małych przedsiębiorstw.

Głębsze kieszenie i ubezpieczenie

Ponieważ większe organizacje mają większe szanse na posiadanie dużych ilości gotówki i aktywów niż małe firmy, są lepszymi celami dla pozwów zbiorowych i różnych innych form procesów sądowych niż sklepy typu mom and pop. Prawnicy nie chcą poświęcać dużej ilości czasu na walkę ze sprawą, jeśli ich osoba docelowa nie ma pieniędzy na rozliczenie lub może zbankrutować (a zatem nie zapłacić) w przypadku orzeczenia. W rezultacie prawdopodobieństwo, że większe przedsiębiorstwo stanie się celem pozwu, jeśli wyciek z niego danych w wyniku naruszenia, jest stosunkowo wysokie w porównaniu z prawdopodobieństwem, że to samo stanie się z dużo mniejszą firmą, która doświadczy podobnego naruszenia.

Z myślą o pracownikach, konsultantach i partnerach

Pracownicy są często najsłabszym ogniwem w łańcuchu bezpieczeństwa firmy. Znacznie bardziej złożone formy zatrudnienia stosowane przez duże przedsiębiorstwa - często obejmujące pracowników związkowych, pracowników niezrzeszonych, bezpośrednio zatrudnianych podwykonawców, wykonawców zatrudnianych za pośrednictwem firm, podwykonawców i tak dalej - grożą jeszcze pogorszeniem problemu w przypadku większych przedsiębiorstw. Jakakolwiek złożoność zwiększa prawdopodobieństwo popełnienia błędów. Ponieważ ludzkie błędy są głównym katalizatorem naruszeń danych, duże przedsiębiorstwa muszą wyjść poza procesy zarządzania ludźmi i procedury małych firm. Muszą na przykład usprawnić procesy decydowania o tym, kto ma dostęp do czego i kto może udzielić upoważnienia na co. Muszą ustanowić proste procesy odwoływania uprawnień z różnych systemów, gdy pracownicy odchodzą, kontrahenci wykonują swoje zadania i tak dalej. Odwołanie dostępu odchodzącym stronom nie jest tak proste, jak wiele osób mogłoby sobie wyobrazić. Pracownik dużej korporacji może na przykład mieć dostęp do wielu niepołączonych systemów danych znajdujących się w wielu różnych lokalizacjach na całym świecie, którymi zarządzają różne zespoły z różnych działów. Mogą w tym pomóc systemy zarządzania tożsamością i dostępem, które centralizują

części procesów uwierzytelniania i autoryzacji, ale wielu dużych przedsiębiorstwom wciąż brakuje kompleksowej centralizacji niezbędnej do unieważnienia dostępu w jednym kroku.

Radzenie sobie z polityką wewnętrzną

Podczas gdy wszystkie firmy zatrudniające więcej niż jednego pracownika mają jakiś element polityki, duże firmy mogą cierpieć z powodu konfliktów między ludźmi i grupami, które są dosłownie motywowane do działania w bezpośredniej opozycji. Na przykład zespół biznesowy może zostać nagrodzony, jeśli dostarczy nowe funkcje produktu przed określoną datą - co może zrobić łatwiej, jeśli skąpi na bezpieczeństwie - podczas gdy zespół ds. Bezpieczeństwa informacji może być zmotywowany do opóźnienia wydania produktu, ponieważ jest motywowany do upewnić się, że nie ma problemów z bezpieczeństwem i nie wprowadzać produktu szybko na rynek.

Oferowanie szkoleń z zakresu bezpieczeństwa informacji

Wszyscy pracownicy powinni rozumieć pewne podstawy bezpieczeństwa informacji. Powinni na przykład wiedzieć, jak unikać cyber-ryzykownych zachowań, takich jak otwieranie załączników i klikanie linków znajdujących się w nieoczekiwanych wiadomościach e-mail, pobieranie muzyki lub filmów z wątpliwych źródeł, niewłaściwe korzystanie z publicznej sieci Wi-Fi do zadań wrażliwych lub kupowanie produktów od nieznane sklepy z cenami „zbyt dobrymi, aby mogły być prawdziwe" i bez publicznie znanego adresu fizycznego. Jednak w dużych firmach większość pracowników nie zna osobiście większości innych pracowników. Taka sytuacja otwiera drzwi dla wszelkiego rodzaju kontaktów społecznych ataki inżynieryjne - fałszywe żądania kierownictwa dotyczące wysłania W2, fałszywe żądania z działu IT dotyczące resetowania haseł i tak dalej. Szkolenie i praktyka, aby upewnić się, że takie ataki nie mogą skutecznie osiągnąć swoich celów, mają kluczowe znaczenie.

Zreplikowane środowiska

Większe firmy często replikują środowiska nie tylko w celu ochrony przed awariami, ale także w celu konserwacji. W związku z tym często mają trzy repliki dla każdego głównego systemu: system produkcyjny (który może być replikowany sam ze względu na nadmiarowość), środowisko programistyczne i środowisko pomostowe do przeprowadzania testów kodu i poprawek.

Patrząc na rolę dyrektora ds. Bezpieczeństwa informacji

Podczas gdy wszystkie firmy potrzebują kogoś, kto ostatecznie będzie odpowiadał za bezpieczeństwo informacji, większe przedsiębiorstwa często mają duże zespoły zajmujące się bezpieczeństwem informacji i potrzebują kogoś, kto może nadzorować wszystkie aspekty zarządzania bezpieczeństwem informacji, a także zarządzać całym personelem zaangażowanym w działania. więc. Osoba ta reprezentuje również funkcję bezpieczeństwa informacji przed kierownictwem wyższego szczebla, a czasami także przed zarządem. Zwykle osobą tą jest dyrektor ds. Bezpieczeństwa informacji (CISO). Chociaż dokładne obowiązki CISO różnią się w zależności od branży, lokalizacji geograficznej, wielkości firmy, struktury korporacyjnej i odpowiednich przepisów, większość ról CISO ma wspólne podstawowe cechy. Ogólnie rzecz biorąc, rola CISO obejmuje nadzorowanie i przyjmowanie odpowiedzialności za wszystkie obszary bezpieczeństwa informacji. W poniższych sekcjach opisano te obszary.

Ogólne zarządzanie programem bezpieczeństwa

CISO jest odpowiedzialny za nadzorowanie programu bezpieczeństwa firmy od A do Z. Ta rola obejmuje nie tylko ustanowienie polityki bezpieczeństwa informacji w przedsiębiorstwie, ale wszystko, co jest potrzebne do zapewnienia, że cele biznesowe można osiągnąć przy pożądanym poziomie zarządzania ryzykiem - coś, co wymaga na przykład regularnego przeprowadzania ocen ryzyka. Chociaż

teoretycznie małe firmy mają również kogoś odpowiedzialnego za całe ich programy bezpieczeństwa, w przypadku dużych przedsiębiorstw programy są zwykle znacznie bardziej formalne, z większą liczbą ruchomych części. Takie programy również trwają bez końca.

Test i pomiar programu bezpieczeństwa

CISO jest odpowiedzialny za ustanowienie odpowiednich procedur testowania i wskaźników sukcesu, w oparciu o które będzie mierzyć skuteczność planu bezpieczeństwa informacji i odpowiednio wprowadzać poprawki. Ustalenie właściwych metryk bezpieczeństwa jest często dużo bardziej skomplikowane, niż można by początkowo przypuszczać, ponieważ zdefiniowanie „pomyślnej wydajności", jeśli chodzi o bezpieczeństwo informacji, nie jest prostą sprawą.

Zarządzanie ryzykiem dla ludzi CISO jest również odpowiedzialny za rozwiązywanie różnych zagrożeń dla ludzi. Sprawdzanie pracowników przed ich zatrudnieniem, definiowanie ról i obowiązków, szkolenie pracowników, dostarczanie pracownikom odpowiednich instrukcji obsługi i przewodników dla pracowników, zapewnianie pracownikom symulacji naruszeń bezpieczeństwa informacji i informacji zwrotnych, tworzenie programów motywacyjnych itd., Wszystko to często wiąże się z udziałem organizacji CISO .

Klasyfikacja i kontrola zasobów informacyjnych

Ta funkcja CISO obejmuje przeprowadzanie inwentaryzacji zasobów informacyjnych, opracowanie odpowiedniego systemu klasyfikacji, klasyfikację aktywów, a następnie decydowanie o rodzajach kontroli (na na poziomie biznesowym), aby odpowiednio zabezpieczyć różne klasy i aktywa. Kontrole i aktywa powinny obejmować audyt i odpowiedzialność. Kontrole powinny również obejmować audyt i odpowiedzialność.

Operacje bezpieczeństwa

Operacje bezpieczeństwa oznaczają dokładnie to, na co wygląda. Jest to funkcja biznesowa, która obejmuje zarządzanie bezpieczeństwem w czasie rzeczywistym, w tym analizę zagrożeń i monitorowanie zasobów technologicznych firmy (systemów, sieci, baz danych itd.) Oraz środków zaradczych w zakresie bezpieczeństwa informacji, takich jak zapory ogniowe, czy hostowane wewnętrznie lub zewnętrznie, ze względu na wszystko, co może być nieprawidłowe. Personel operacyjny to także osoby, które początkowo reagują, jeśli stwierdzą, że coś poszło nie tak.

Strategia bezpieczeństwa informacji

Ta rola obejmuje opracowanie przyszłościowej strategii bezpieczeństwa firmy, aby zapewnić firmie bezpieczeństwo w przyszłości. Proaktywne planowanie i działanie jest o wiele bardziej pocieszające dla akcjonariuszy niż reagowanie na ataki.

Zarządzanie tożsamością i dostępem

Ta rola dotyczy kontrolowania dostępu do zasobów informacyjnych w oparciu o wymagania biznesowe i obejmuje zarządzanie tożsamością, uwierzytelnianie, autoryzację i powiązane monitorowanie. Obejmuje wszystkie aspekty firmowych zasad i technologii zarządzania hasłami, wszelkie zasady i systemy uwierzytelniania wieloskładnikowego oraz wszelkie systemy katalogowe, które przechowują listy osób i grup oraz ich uprawnienia. Zespoły CISO ds. Tożsamości i zarządzania dostępem są odpowiedzialne za zapewnienie pracownikom dostępu do systemów niezbędnych do wykonywania ich pracy oraz za cofnięcie takiego dostępu, gdy pracownik odchodzi. Podobnie zarządzają dostępem partnerów i wszystkimi innymi dostępami zewnętrznymi. Duże korporacje prawie zawsze korzystają z formalnych systemów usług katalogowych - na przykład Active Directory jest dość popularny.

Zapobieganie utracie danych

Zapobieganie utracie danych obejmuje zasady, procedury i technologie, które zapobiegają wyciekowi zastrzeżonych informacji. Mogą wystąpić wycieki przypadkowo - na przykład użytkownik może przypadkowo dołączyć niewłaściwy dokument do wiadomości e-mail przed wysłaniem wiadomości - lub pod wpływem złej woli (na przykład niezadowolony pracownik kradnie cenną własność intelektualną, kopiując ją na dysk USB i zabierając dysk do domu tuż przed skopiowanie go na dysk USB i zabranie go do domu tuż przed rezygnacją). W ostatnich latach niektóre funkcje zarządzania mediami społecznościowymi zostały przeniesione do grupy zapobiegania utracie danych. Przecież nadmierne udostępnianie w mediach społecznościowych często obejmuje faktyczne udostępnianie przez pracowników informacji, których firmy nie chcą udostępniać w publicznie dostępnych sieciach społecznościowych.

Zapobieganie oszustwom

Niektóre formy zapobiegania oszustwom często należą do domeny CISO. Na przykład, jeśli firma prowadzi witryny internetowe przeznaczone dla konsumentów, które sprzedają produkty, często do obowiązków CISO należy zminimalizowanie liczby oszukańczych transakcji dokonywanych w tych witrynach. Nawet jeśli taka odpowiedzialność nie wchodzi w zakres kompetencji CISO, CISO prawdopodobnie będzie zaangażowany w ten proces, ponieważ systemy przeciwdziałania oszustwom i systemy bezpieczeństwa informacji często korzystają wzajemnie z wymiany informacji o podejrzanych użytkownikach. Oprócz zajmowania się zwalczaniem oszukańczych transakcji, CISO może być odpowiedzialny za wdrażanie technologii uniemożliwiających nieuczciwym pracownikom kradzież pieniędzy z firmy za pośrednictwem jednego lub kilku z wielu rodzajów schematów - przy czym CISO zwykle koncentruje się głównie na środkach związanych z komputerami.

Plan reagowania na incydenty

CISO jest odpowiedzialny za opracowanie i utrzymanie planu reagowania na incydenty firmy. Plan powinien obejmować nie tylko kroki techniczne opisane w rozdziałach 11 i 12, ale także szczegóły, kto rozmawia z mediami, kto czyści wiadomości z mediami, kto informuje opinię publiczną, kto informuje organy regulacyjne, kto konsultuje się z organami ścigania itd. . Powinien również szczegółowo określać tożsamości (określone przez opis stanowiska) i role wszystkich innych decydentów w procesie reagowania na incydenty. Odzyskiwanie po awarii i planowanie ciągłości działania.

Ta funkcja obejmuje zarządzanie zakłóceniami normalnej działalności poprzez planowanie awaryjne i testowanie wszystkich takich planów. Podczas gdy duże firmy często mają oddzielny zespół DR i BCP, CISO prawie zawsze odgrywa główną rolę w tych funkcjach - jeśli nie jest ich bezpośrednim właścicielem - z wielu powodów:

* Udostępnianie systemów i danych jest częścią obowiązków CISO. W związku z tym z praktycznego punktu widzenia jest niewielka różnica, jeśli system ulegnie awarii, ponieważ plan DR i BC jest nieskuteczny lub z powodu ataku DDoS - jeśli systemy i dane nie są dostępne, jest to problem CISO.

* CISO muszą upewnić się, że plany BCP i DR przewidują odzyskiwanie w taki sposób, aby zachować bezpieczeństwo. Jest to szczególnie prawdziwe, ponieważ często z doniesień prasowych wynika, że duże korporacje mogą potrzebować aktywować swoje plany ciągłości, a hakerzy wiedzą, że firmy w trybie odzyskiwania stanowią idealne cele.

Spełnienie

CISO jest odpowiedzialny za zapewnienie, że firma przestrzega wszystkich wymogów prawnych i regulacyjnych, zobowiązań umownych i najlepszych praktyk zaakceptowanych przez firmę w zakresie bezpieczeństwa informacji. Oczywiście eksperci ds. Zgodności i prawnicy mogą doradzać CISO w takich sprawach, ale ostatecznie obowiązkiem CISO jest zapewnienie spełnienia wszystkich wymagań.

Dochodzenia

Jeśli (i kiedy) dojdzie do incydentu związanego z bezpieczeństwem informacji, osoby pracujące dla CISO w tym charakterze badają, co się stało. W wielu przypadkach będą to osoby, które koordynują dochodzenia z organami ścigania, firmami konsultingowymi, organami regulacyjnymi lub zewnętrznymi firmami ochroniarskimi. Zespoły te muszą posiadać umiejętności w zakresie kryminalistyki i zabezpieczania dowodów. Niewiele dobrze jest wiedzieć, że jakiś nieuczciwy pracownik ukradł pieniądze lub dane, jeśli w wyniku niewłaściwego postępowania z dowodami cyfrowymi nie możesz udowodnić w sądzie, że tak jest.

Bezpieczeństwo fizyczne

Zapewnienie fizycznego bezpieczeństwa korporacyjnych zasobów informacyjnych jest częścią zadania CISO. Obejmuje to nie tylko systemy i sprzęt sieciowy, ale także transport i przechowywanie kopii zapasowych, utylizację wycofanych komputerów i tak dalej. W niektórych organizacjach CISO jest również odpowiedzialny za fizyczne bezpieczeństwo technologii mieszkaniowej budynków i przebywających w nich ludzi. Niezależnie od tego, czy tak jest, CISO jest zawsze odpowiedzialny za współpracę z osobami odpowiedzialnymi w celu zapewnienia, że systemy informacyjne i dane współpracują z osobami odpowiedzialnymi w celu zapewnienia, że systemy informacyjne i magazyny danych są chronione za pomocą odpowiednio zabezpieczonych obiektów posiadających odpowiednie granice bezpieczeństwa i odpowiednie kontrola dostępu do wrażliwych obszarów w zależności od potrzeby dostępu.

Architektura bezpieczeństwa

CISO i jego zespół są odpowiedzialni za projektowanie i nadzorowanie budowy i utrzymania architektury bezpieczeństwa firmy.

Oczywiście czasami CISO dziedziczą elementy infrastruktury, więc zakres, w jakim mogą projektować i budować, może się różnić. CISO skutecznie decyduje, co, gdzie, jak i dlaczego stosuje się różne środki zaradcze, jak projektować topologię sieci, strefy DMZ i segmenty, i tak dalej.

Zapewnienie audytowalności administratorów systemu

Obowiązkiem CISO jest zapewnienie, aby wszyscy administratorzy systemu rejestrowali swoje działania w taki sposób, aby ich działania podlegały audytowi i można je było przypisać stronom, które je podjęły.

Zgodność z cyberbezpieczeństwem

Większość dużych firm posiada ubezpieczenie cyberbezpieczeństwa. Zadaniem CISO jest upewnienie się, że firma spełnia wszystkie wymagania dotyczące ochrony ubezpieczeniowej w ramach obowiązujących polis, tak aby jeśli coś pójdzie nie tak i zostanie zgłoszone roszczenie, firma zostanie objęta ubezpieczeniem.