ZABEZPIECZANIE NARZĘDZI P2P, IM, SMS I WSPÓŁPRACA

WPROWADZENIE.

Komunikacja peer-to-peer (P2P), wiadomości błyskawiczne (IM), obsługa krótkich wiadomości (SMS) i narzędzia współpracy muszą być bezpośrednio uwzględnione w każdym kompleksowym planie bezpieczeństwa. Zagrożenia są realne, podobnie jak prawdopodobieństwo, że przynajmniej jedna z tych technologii jest używana w prawie każdej organizacji.

OGÓLNE POJĘCIA I DEFINICJE.

Ten rozdział ma na celu przedstawienie wystarczającej ilości informacji i zasobów, aby pomóc w zintegrowaniu obrony każdej funkcji z planem bezpieczeństwa organizacji. Lista zasobów znajduje się na końcu rozdziału, aby pomóc w dalszych badaniach.

Peer to Peer.

Sieci peer-to-peer, określane również jako P2P, nie są nową koncepcją ani technologią. Termin ten był zawarty w niektórych oryginalnych projektach i propozycjach dotyczących Internetu jako wydajnego i logicznego sposobu wymiany informacji z jednego zasobu lub równorzędnego do drugiego w dużej połączonej sieci. Obecnie termin ten jest najbardziej kojarzony z aplikacjami, które przesyłają pliki multimedialne przez Internet. Sieci peer-to-peer zazwyczaj składają się z różnych komputerów lub węzłów, które komunikują się bezpośrednio ze sobą, często z niewielką, jeśli w ogóle, potrzebą centralnego komputera do kontrolowania aktywności. Często wykorzystując aplikację o wyglądzie klient-serwer, dwa komputery ustanawiają między sobą bezpośrednie połączenie w celu przesyłania plików. Centralny komputer indeksujący może, ale nie musi być potrzebny, aby pomóc tym komputerom „odnajdywać się" nawzajem, indeksować i publikować ich zawartość lub ułatwiać połączenie. Jednak co najważniejsze, oba komputery muszą mieć bezpośrednie, logiczne połączenie, aby przesłać plik lub pliki. Transport plików może odbywać się przez sieć lokalną (LAN), sieć rozległą (WAN), sieć o wartości dodanej (VAN) lub przez Internet. Technologie i aplikacje peer-to-peer były znacznie bardziej rozpowszechnione we wczesnych dniach sieci, kiedy dla wielu organizacji posiadanie drogich serwerów i skomplikowanych topologii sieci nie było finansowo możliwe. Dotyczy to zwłaszcza osobistych sieci komputerowych, które przeprowadzały proste udostępnianie plików z komputera na komputer w modelu jeden-do-jednego, zamiast dzisiejszej znacznie bardziej powszechnej konfiguracji jeden-do-wielu serwer-klient. Istnieją jednak uzasadnione zastosowania technologii peer-to-peer. Jednym z typowych przykładów jest udostępnianie obrazów oprogramowania do dystrybucji Linuksa. Udostępnianie w trybie peer-topeer tych często dużych obrazów dysków ISO wymaga znacznie mniejszych zasobów dla dystrybutora, ponieważ mogą istnieć tysiące komputerów, które dystrybuują oprogramowanie między sobą, a nie każdy użytkownik próbujący pobrać plik z jednego serwera.

Wiadomości błyskawiczne.

Wiadomości błyskawiczne (IM) stały się jednym z najczęściej używanych środków komunikacji i szybko wyprzedza pocztę elektroniczną jako preferowaną technologię do komunikowania się z innymi. To narzędzie pozwala użytkownikom komunikować się ze sobą w czasie rzeczywistym, synchronicznie, natychmiastowo za pośrednictwem komputera, tabletu lub urządzenia mobilnego. Dzisiejsze aplikacje IM nie zbliżają się do pierwszej generacji IM. Koncepcja komunikowania się lub czatowania w czasie rzeczywistym pojawiła się w systemach komputerowych z wieloma użytkownikami, kiedy użytkownicy mogli inicjować ze sobą konwersację tekstową. Najczęstszym przykładem tego typu komunikacji był system oparty na hoście, taki jak środowisko mainframe lub system UNIX, wykorzystujący programy takie jak talk lub ytalk. Początkowo użytkownicy mogli być ograniczeni do komunikowania się ze sobą,

gdy byli zalogowani na tym samym komputerze; ostatecznie użytkownicy byli w stanie komunikować się ze sobą za pośrednictwem Internet Relay Chat (IRC) lub za pośrednictwem wczesnych usług internetowych, takich jak America Online. Pierwsze powszechne zastosowania komunikatorów internetowych stały się możliwe dzięki popularności komputera PC z modemem i były wykorzystywane głównie do krótkich, nieformalnych, osobistych rozmów. Z czasem komunikatory internetowe stały się narzędziem biznesowym, aw niektórych organizacjach wręcz koniecznością, zwłaszcza dla telepracowników. Konieczność komunikowania się ze współpracownikami, sprzedawcami, klientami, klientami itp. przekształciła sztuczną technologię w wszechobecność. Wraz z tą zmianą konieczne jest, aby zarządzanie bezpieczeństwem zmieniło się i odpowiednio dostosowało. Użytkownicy mogą wysyłać wiadomości, pliki, strumieniować wideo i audio w czasie rzeczywistym, korzystać z internetowych tablic do współpracy i udostępniać pulpity niemal natychmiast. Niezbędne dla organizacji lub nie, komunikatory internetowe mogą stać się niebezpiecznym nośnikiem naruszeń bezpieczeństwa.

Usługa krótkich wiadomości.

Usługa krótkich wiadomości, lub częściej SMS, to kolejna wcześniej niewielka technologia, która stała się wszechobecna i stanowi dużą część codziennego życia wielu ludzi. Chociaż niektóre standardy telefonii komórkowej i firmy miały różne pomysły na wykorzystanie SMS-ów, powszechnym wczesnym zastosowaniem było powiadamianie klientów o informacjach w jedną stronę, od operatora telefonii komórkowej do użytkownika. Popularnym przykładem było powiadamianie użytkownika o nieodebranym połączeniu lub wiadomości na poczcie głosowej. Wielu przewoźników nigdy nie śniło, że klienci będą mogli wysyłać wiadomości tekstowe z jednego telefonu komórkowego na drugi, ani też operatorzy nie sądzili, że użytkownicy kiedykolwiek będą chcieli robić coś takiego. Nazwa, usługa krótkich wiadomości, również sugerowała ograniczoną ilość tekstu, jaką może zawierać wiadomość. Pierwotnie użytkownicy byli ograniczeni do 160 znaków lub mniej. SMS przekształcił się w coś znacznie większego. Powszechność telefonów komórkowych sprawiła, że pierwotna koncepcja znacznie przekroczyła jej pierwotne znaczenie i funkcję. Obecnie dwustronna komunikacja między klientami telefonii komórkowej, często w sieciach różnych operatorów telefonii komórkowej, między klientami a operatorami telefonii komórkowej oraz między klientami a innymi systemami informatycznymi, stała się sposobem na życie. Klienci oczekują natychmiastowych, zawsze aktywnych i niezawodnych usług SMS. Większość telefonów komórkowych umożliwia wysyłanie wiadomości tekstowych SMS, robienie i wysyłanie zdjęć, natychmiastowe powiadomienia oraz szereg innych usług, które wykorzystują lub rozszerzają pierwotną koncepcję usług krótkich wiadomości.

Narzędzia do współpracy.

Osoby pracujące razem stworzyły zapotrzebowanie na jeszcze więcej technologii, które pomogą im w wykonywaniu ich zadań. Na dzisiejszym rynku istnieje wiele produktów ułatwiających udostępnianie, współpracę i organizację danych. Jak żartują niektórzy specjaliści ds. bezpieczeństwa informacji: „Komputery i technologia są ogólnie bezpieczne, dopóki nie pozwolisz człowiekowi się do nich zbliżyć". Ludzie są nieuniknieni, jeśli chodzi o narzędzia i systemy współpracy. Wiele narzędzi i systemów do współpracy zostało zaprojektowanych z myślą o wsparciu grup roboczych, które są fizycznie od siebie oddalone. Gdy system ma wymagania, które zawierają słowa „otwarty", „przez Internet" lub „dostęp z dowolnego miejsca", specjaliści ds. bezpieczeństwa informacji kulą się. Zabezpieczanie narzędzi do współpracy może być trudne, zwłaszcza jeśli chodzi o zrównoważenie funkcjonalności i bezpieczeństwa. Podręcznik nie byłby kompletny, gdyby pominięto chmurę, a właśnie tam znajduje się większość obecnych narzędzi do współpracy, w tym ich dane. Narzędzia te powodują również przeciąganie liny między użytkownikami a specjalistami ds. bezpieczeństwa - użytkownicy chcą z nich korzystać; specjaliści od bezpieczeństwa martwią się konsekwencjami. Usługi udostępniania plików,

takie jak Dropbox i Google Docs, dołożyły starań, aby zabezpieczyć dane przechowywane i udostępniane przez osoby i grupy. Na przykład Dropbox odpowiada na pytanie „Jak bezpieczny jest Dropbox?" następująco:

Mamy dedykowany zespół ds. bezpieczeństwa, który wykorzystuje najlepsze dostępne narzędzia i praktyki inżynieryjne do tworzenia i utrzymywania Dropbox. Możesz mieć pewność, że wdrożyliśmy wiele poziomów zabezpieczeń, aby chronić Twoje pliki i tworzyć ich kopie zapasowe. Możesz także skorzystać z weryfikacji dwuetapowej, funkcji uwierzytelniania logowania, którą możesz włączyć, aby dodać kolejną warstwę bezpieczeństwa do swojego konta. Inni użytkownicy Dropbox nie widzą Twoich plików w Dropbox, chyba że celowo udostępnisz łącza do plików lub udostępnisz foldery. Pracownikom Dropbox nie wolno przeglądać zawartości plików przechowywanych na Twoim koncie. Pracownicy mogą uzyskiwać dostęp do metadanych plików (np. nazw i lokalizacji plików), gdy mają uzasadniony powód, np. zapewnienie pomocy technicznej. Podobnie jak większość usług online, mamy niewielką liczbę pracowników, którzy muszą mieć dostęp do danych użytkownika z powodów określonych w naszej polityce prywatności (np. gdy jest to prawnie wymagane). Ale to rzadki wyjątek, a nie reguła. Stosujemy surowe zasady i techniczne kontrole dostępu, które zabraniają dostępu pracownikom, z wyjątkiem tych rzadkich okoliczności. Ponadto stosujemy szereg fizycznych, technicznych i heurystycznych środków bezpieczeństwa w celu ochrony informacji użytkownika przed nieautoryzowanym dostępem.

Niemniej jednak istnieją poważne obawy dotyczące bezpieczeństwa narzędzi do udostępniania plików w chmurze, a w szczególności Dropbox. Na konferencji Black Hat EU w 2013 r. uwagę pisarza Michaela Kassnera przyciągnął artykuł „DropSmack: Jak usługi synchronizacji w chmurze czynią twoją korporacyjną zaporę sieciową bezwartościową". Streszczenie artykułu zawierało następujące punkty:

* „… Rozwiązania synchronizacji oparte na [C]loud ogólnie, a Dropbox w szczególności, mogą być wykorzystywane jako wektor do dostarczania złośliwego oprogramowania do sieci wewnętrznej".

* „… usługa synchronizacji Dropbox może być używana jako kanał dowodzenia i kontroli (C2)."

* „… [F]funkcjonujące złośliwe oprogramowanie może używać Dropbox do przemycania danych z eksploatowanych komputerów zdalnych".

Autor artykułu, doświadczony tester penetracji Jacob Williams, ostrzegł, że jeśli zły aktor ma jakikolwiek dostęp do zabezpieczonego folderu Dropbox, możliwe jest zsynchronizowanie stworzonego przez niego trojana zdalnego dostępu o nazwie DropSmack ze wszystkimi współdzielonymi folderami Dropbox. Narzędzie umożliwiłoby infiltrację całej sieci korporacyjnej. Williams ostrzegł również, że dostęp do folderu Dropbox przez pracowników korzystających z ich komputerów osobistych rodzi problemy prawne:

Wielu doradców generalnych jest bardziej niż trochę zaniepokojonych pojawieniem się upoważnienia nas do testu piórkowego, który może być komputerami domowymi. W dzisiejszych czasach staje się to trudnym problemem dla testerów piórkowych, ponieważ ludzie otwierają wiadomości e-mail typu spear phishing dostarczane na firmowe adresy e-mail na komputerach, które mogą być własnością prywatną.

Zintegrowane narzędzia do współpracy niosą ze sobą jeszcze jedno niebezpieczeństwo, szczególnie dla niedoświadczonych użytkowników, którzy nie wykonują codziennych kopii zapasowych: usunięcie jednego lub więcej plików (lub wszystkich) z udostępnionego folderu Dropbox rozprzestrzeni je na wszystkich użytkowników folderu udostępnionego. Jeśli któryś z użytkowników prowadzi codzienną kopię zapasową, cała grupa użytkowników może być chroniona przed katastrofą; jeśli żaden z nich tego

nie zrobi, mogą mieć poważne trudności. W powiązanym problemie każdy użytkownik, który przeniesie pliki z folderu Dropbox do folderu lokalnego, usunie dane również ze wszystkich folderów Dropbox innych użytkowników. W artykule z 2012 r. Matthew J. Schwartz wezwał użytkowników korporacyjnych do zwrócenia uwagi na korzystanie z Dropbox przez swoich pracowników. Jego pięć rekomendacji (więcej szczegółów w oryginalnym artykule) to:

1. Monitoruj korzystanie z Dropbox

2. Porównaj zabezpieczenia usług w chmurze

3. Uważaj na słabe praktyki bezpieczeństwa w chmurze

4. Traktuj Dropbox jako publiczne repozytorium

5. Uważaj na eksfiltrację danych wewnętrznych4

Darmowe narzędzie Cloudfogger automatycznie szyfruje dane po stronie klienta, gdy są one przesyłane do dowolnego zewnętrznego narzędzia do współpracy przy użyciu 256-bitowego szyfrowania AES. Narzędzie automatycznie odszyfrowuje dane po pobraniu przez autoryzowanego użytkownika

SIECI PEER-TO-PEER.

Jednym z pierwszych masowych zastosowań P2P było bezpłatne udostępnianie plików muzycznych za pośrednictwem Napster, LLC. Pomimo trudności związanych z prawami autorskimi i późniejszego bankructwa, technologia Napstera, w zasadniczo tej samej formie, jest nadal w powszechnym użyciu. Praktyczne zastosowania rozszerzyły się poza pobieranie muzyki do świata biznesu, na przykład umożliwiając udostępnianie małym grupom użytkowników pliki bez interakcji administratora systemu i dystrybucji oprogramowania open source. Podobnie może się zdarzyć, że pracownicy będą korzystać z szybkiego połączenia internetowego organizacji, aby uzupełnić swoją kolekcję filmów w domu za pośrednictwem P2P.

Zagrożenia dla firmy.

Korzystając z technologii P2P bez odpowiedniej opieki i kontroli, organizacja może ponieść poważne konsekwencje. Istnieje wiele zagrożeń dla organizacji, która nie kontroluje prawidłowo sieci P2P, tak jak w przypadku każdej innej konfiguracji sieci lub protokołu. Wiele problemów omówiono w rozdziałach 21, 25 i 26 niniejszego Podręcznika. Jednak ta sekcja zawiera kilka ważnych kwestii, które zarządzanie bezpieczeństwem informacji powinno wziąć pod uwagę podczas przeprowadzania analizy ryzyka i wdrażania polityki dla sieci P2P.

Nadużywanie zasobów firmy i nielegalnych treści.

Organizacje muszą mieć akceptowalną politykę użytkowania, która ogranicza to, co pracownicy mogą zrobić z udostępnionymi im zasobami technologicznymi. Polityka powinna jasno określać rodzaje technologii i aplikacji, które są zabronione lub ograniczone w określony sposób. W większości przypadków technologia P2P używana do pobierania muzyki lub filmów do użytku osobistego narusza zasady. Technologia P2P stanowi szczególne zagrożenie dla zasobów technologicznych firmy, ponieważ nieodłączną naturą technologii P2P jest wykorzystanie każdego zasobu w maksymalnym możliwym stopniu. Na przykład pojedyncza aplikacja P2P, poprawnie skonfigurowana, będzie wykorzystywać każdy bit przepustowości, który jest dla niej dostępny. Obejmuje to przepustowość sieci LAN, przepustowość sieci WAN i przepustowość Internetu. Jednym z najpopularniejszych zastosowań technologii P2P nadal pozostaje udostępnianie bardzo dużych plików, zwłaszcza plików multimedialnych, w tym filmów pełnometrażowych. Pełne pobranie tych dużych plików może zająć

kilka godzin. Fakt ten może mieć niezwykle negatywny wpływ na infrastrukturę sieciową organizacji, w tym na kosztowną przepustowość Internetu. W praktyce wykazano, że pojedyncza aplikacja P2P całkowicie nasyca 12-megabitowe połączenie internetowe, praktycznie uniemożliwiając lub poważnie ograniczając dostęp do wszystkich innych komputerów.6 W tym przypadku te zagrożenia dla firmy są wspólne dla wielu obszarów informacji zarządzanie bezpieczeństwem:

* Zagrożenie dostępności. Jeśli zasoby organizacji, w tym zasoby sieciowe, nie są dostępne, firma nie może prawidłowo funkcjonować.

* Zagrożenie dla integralności. Jeśli zasoby organizacji są sparaliżowane lub wykorzystywane przez pracowników korzystających z technologii P2P, dane mogą ucierpieć z powodu naruszenia integralności i użyteczności.

* Zagrożenie wizerunku organizacji. Jeśli nie można polegać na systemach informatycznych i infrastrukturze organizacji z powodu przerw spowodowanych nadużyciami P2P, istnieje ryzyko pogorszenia wizerunku finansowego lub publicznego. Niektóre organizacje nie są w stanie przezwyciężyć znacznej utraty wizerunku, wiarygodności lub obu.

* Zagrożenie z postępowania sądowego. Często zdarza się, że nielegalne treści są udostępniane za pośrednictwem technologii P2P; nielegalne udostępnianie muzyki i filmów często przypisuje się popularyzacji technologii P2P. Organizacja może mieć problemy prawne, w tym pozwy dotyczące praw autorskich i własności intelektualnej, jeśli jej zasoby są zaangażowane w udostępnianie nielegalnych materiałów. Niektóre grupy antypirackie stały się niezwykle agresywne w zwalczaniu nielegalnego udostępniania treści chronionych prawem autorskim.

Utrata poufności.

Istnieje wiele sposobów, w jakie organizacja może stracić poufność z powodu technologii P2P. Jednym z powszechnych błędów jest źle skonfigurowana aplikacja P2P. Studium przypadku w sekcji 35.3.4 opisuje jedną sytuację. Jednak zagrożenia związane z błędnie skonfigurowaną aplikacją P2P są realne – dość łatwo jest nieumyślnie udostępnić dane. Gdy użytkownicy się spieszą lub nie rozumieją, co robią, aplikacja P2P może pozwolić na nieautoryzowany dostęp do informacji, ponieważ jej ograniczenia są zbyt luźne lub całkowicie ich brakuje. Częstym błędem w środowisku Microsoft Windows może być udostępnianie całego folderu „Moje dokumenty”, gdy użytkownik zamierza udostępniać tylko zdjęcia. Źle skonfigurowana lub złośliwie zmieniona aplikacja P2P może również stać się kanałem lub punktem dostępu, w którym atakujący może wejść do innego bezpiecznego środowiska sieciowego. Innym, mniej znanym i często pomijanym zagrożeniem jest ilość danych, które aplikacja P2P może ujawnić osobom nieupoważnionym. Na przykład aplikacja P2P może oferować szczegółowe informacje o swoim hoście, w tym:

* System operacyjny, wersja i konfiguracja

* Schemat adresu sieci korporacyjnej, konwencja nazewnictwa hostów, informacje DNS

* Szczegółowe informacje o wersji lub kompilacji aplikacji P2P (przydatne dla atakujących w celu wykorzystania znanych luk w „błędnym” wydaniu lub wersji)

* Trasy sieciowe, uprzywilejowany dostęp z określonego komputera do wrażliwych sieci w organizacji (za zaporą itp.)

* Otwórz porty sieciowe w zaporze sieciowej organizacji

Chociaż wiele z tych przykładów może wydawać się same w sobie raczej łagodne, aplikacja P2P może ujawniać informacje, które atakujący może wykorzystać w ramach większego ataku. Rozdział 19 niniejszego podręcznika szczegółowo opisuje, w jaki sposób można gromadzić i wykorzystywać razem małe fragmenty informacji w przypadku naruszenia bezpieczeństwa informacji. Charakter i funkcjonalność aplikacji P2P ujawnia poufne informacje, które w przeciwnym razie nie zostałyby ujawnione. Wszystkie aplikacje P2P nie są sobie równe; aplikacja P2P może różnić się od oczekiwań użytkownika. Czy aplikacja P2P może być rzeczywiście niezawodną, wolną od złośliwego oprogramowania i bezpieczną aplikacją – zwłaszcza, gdy aplikacja jest pobierana bezpłatnie z Internetu? Możliwe, że exploit backdoora, złośliwe oprogramowanie, oprogramowanie szpiegujące lub tym podobne mogą zostać wbudowane w aplikację P2P lub wprowadzone później. Było to szczególnie prawdziwe w czasach Napstera; wiele aplikacji zawierało niechciane złośliwe oprogramowanie, od niewinnego do wręcz niebezpiecznego. Podobne exploity są nadal możliwe. Wielu użytkowników nadal nie do końca rozumie funkcjonalność aplikacji. To, co może zacząć się, gdy użytkownik próbuje pobrać pojedynczy film, może przekształcić się w aplikację, która nigdy nie zostanie odinstalowana i zawsze działa, przesyła lub „wysyła" ten pojedynczy film przez tygodnie lub miesiące. Ponieważ wiele z tych aplikacji jest zbudowanych tak, aby działały cicho w tle, użytkownik może pomyśleć, że film został pobrany, a aplikacja nie jest już używana, podczas gdy w rzeczywistości nadal działa, dopóki nie zostanie usunięta. Jest to nie tylko marnowanie zasobów, ale prawdopodobny sposób na narażenie organizacji na skargę DMCA (Digital Millennium Copyright Act) ze strony organizacji, która jest właścicielem własności intelektualnej.

Konsekwencje.

Każda organizacja, która nie chroni przed utratą danych za pośrednictwem sieci P2P, jest narażona na duże ryzyko publicznego ujawnienia i kontroli, kar finansowych, kar regulacyjnych i tak dalej. Funkcjonalność i charakter aplikacji P2P może dostarczyć badaczowi lub, co gorsza, prasie ostatecznych dowodów na wykorzystanie technologii P2P w organizacji. (Łatwo jest odkryć organizację, która ma użytkowników korzystających z aplikacji P2P, ponieważ istnieje kilka internetowych baz danych adresów IP zarejestrowanych podczas uczestnictwa w „ulu" P2P). Większość społeczeństwa może rozumieć tylko technologie P2P, których należy używać w połączeniu nielegalne udostępnianie muzyki; nawet to proste, negatywne postrzeganie może mieć ogromny wpływ na opinię publiczną o organizacji. Trudno byłoby obalić analizę pakietów lub zrzuty ekranu zawierające adres IP organizacji, w której komputer został włamany, wykorzystany do nielegalnego oprogramowania lub udostępniania multimediów lub komputer był używany przez nieautoryzowany podmiot do wyodrębnienia danych. W dobie aplikacji P2P powszechnie wykorzystywanych do nielegalnego udostępniania i rozpowszechniania własności intelektualnej niechętnych uczestników organizacje podejmują agresywne kroki w celu znalezienia i ścigania przestępców. Rozdział 55 niniejszego Podręcznika zawiera omówienie dochodzeń cybernetycznych; patrz Rozdział 61, aby uzyskać wskazówki dotyczące pracy z organami ścigania.

Zapobieganie i łagodzenie.

Ochrona organizacji przed naruszeniami bezpieczeństwa informacji za pomocą technologii P2P jest jedną z wielu ważnych części ogólnego planu bezpieczeństwa. W zależności od struktury organizacji, przywództwa, funkcji i podobnych czynników, metody zapobiegania i łagodzenia zagrożeń P2P mogą być proste lub skomplikowane. Oczywiście każda organizacja musi przeprowadzić analizę ryzyka i określić swój próg zagrożenia, jeśli chodzi o technologię P2P. Rozdział 62 zawiera środki oceny ryzyka. Poniższe wytyczne mogą pomóc organizacji w obronie przed zagrożeniem ze strony technologii P2P powodującym naruszenia bezpieczeństwa.

Polityka.

Ważne jest, aby każda organizacja zajęła się wykorzystaniem technologii P2P w polityce, takiej jak polityka dopuszczalnego użytkowania, polityka HR lub polityka bezpieczeństwa. Odpowiednia polityka, wraz ze wszystkimi innymi politykami związanymi z bezpieczeństwem, powinna być jasno określona, jasno zakomunikowana całej organizacji, jednolicie i jednakowo egzekwowana oraz aktualizowana w razie potrzeby.

Całkowity zakaz korzystania z technologii peer-to-peer.

W większości przypadków organizacja może całkowicie zakazać korzystania z P2P, zwłaszcza poprzez egzekwowalne zasady. Należy zadbać o to, aby wszyscy pracownicy i komputery przestrzegali zakazu. Powinno być zabronione, a nawet lepiej niemożliwe, instalowanie aplikacji P2P na komputerach osobistych, serwerach i wszystkich innych systemach informatycznych, które mogłyby być używane do wysyłania i odbierania ruchu związanego z P2P. Większość użytkowników komputerów powinna działać jako standardowy użytkownik swojego komputera, a nie jako administrator. Jeśli pracownicy mogą instalować oprogramowanie lub mają dostęp administracyjny do swoich pulpitów, powinny mieć miejsce regularne, zautomatyzowane inwentaryzacje i audyty komputerów. Usunięcie powinno być natychmiastowe i należy podjąć odpowiednie działania naprawcze. Kilka technologii może również pomóc w blokowaniu ruchu P2P, chociaż żadne rozwiązanie technologiczne nie jest całkowicie niezawodne. Środki te są dodatkowymi zabezpieczeniami, a nie kompletnymi rozwiązaniami. Zapory powinny być skonfigurowane z domyślną zasadą odmowy i powinny zezwalać na przechodzenie tylko portów TCP/IP, które są niezbędne do normalnych operacji biznesowych. Chociaż wiele aplikacji P2P jest w stanie tunelować przez porty TCP/IP, takie jak te używane przez HTTP lub inne popularne protokoły, jest to niezbędna pierwsza obrona. Technologie kształtowania pakietów mogą być również przydatne do identyfikowania ruchu związanego z P2P i blokowania jego komunikacji. Urządzenia do kształtowania pakietów i zarządzania ruchem często są w stanie wykryć sygnaturę ruchu P2P, bez względu na port TCP/IP, z którego korzysta aplikacja. Niektóre systemy wykrywania i zapobiegania włamaniom mogą również identyfikować i blokować ruch P2P, podobnie jak wiele urządzeń filtrujących Internet. Dzienniki i raporty powinny być sprawdzane codziennie, a wykroczenia powinny być szybko naprawiane. Jest to również przypadek, w którym ważne jest zarządzane środowisko pulpitu — automatyczna instalacja/usuwanie oprogramowania, jednolite obrazowanie pulpitu oraz zautomatyzowana inwentaryzacja/raportowanie oprogramowania pomaga administratorom komputerów stacjonarnych w zwalczaniu instalowanego oprogramowania P2P wbrew zasadom.

Bezpieczeństwo informacji i audyty systemów informatycznych.

Wszystkie systemy informacyjne i komponenty powinny być poddawane audytowi (zarówno zgodnie z harmonogramem, jak i poprzez losowe audyty), aby upewnić się, że nie są skonfigurowane, celowo lub nieumyślnie, do udziału w udostępnianiu plików P2P. Zadanie to powinno być częścią regularnych procesów audytu systemów informatycznych i bezpieczeństwa informacji w każdej organizacji. Jeśli to możliwe, najbardziej przydatne są zewnętrzne i neutralne zasoby, aby zapewnić, że wszystkie systemy są kontrolowane w jednolity, dokładny, powtarzalny i obiektywny sposób.

Uprawnione wykorzystanie biznesowe musi być zarządzane.

Są chwile, kiedy organizacja nie chce całkowicie zakazać lub zablokować korzystania z technologii P2P. Jednym z coraz bardziej powszechnych i uzasadnionych przykładów dla P2P jest dystrybucja oprogramowania typu open source lub aktualizacje za pośrednictwem BitTorrenta. BitTorrent to oparty na P2P protokół do dystrybucji danych — często dużych ilości danych. Szerokie zastosowanie obejmuje dystrybucję kilku dystrybucji systemu operacyjnego Linux. Instalacja systemu Linux często

wiąże się z uzyskaniem obrazów CD-ROM lub DVD w celu utworzenia dysków instalacyjnych. Korzystając z technologii BitTorrent, dostawcy oprogramowania i dystrybutorzy są w stanie dostarczać swoim klientom duże ilości danych bez ponoszenia całego ciężaru dystrybucji, przepustowości i zasobów obliczeniowych. Jednak organizacja musi zarządzać sposobem wykorzystania tej technologii, aby zapewnić, że zasoby nie są nadużywane, a aplikacje P2P są wykorzystywane wyłącznie do dozwolonych, legalnych celów. Można to osiągnąć za pomocą zasad, audytu oraz różnych technologii dostępu do sieci i kontroli. Każda organizacja musi zdefiniować swój własny poziom akceptowalnego ryzyka dla legalnego korzystania z technologii P2P i musi znaleźć rozwiązania, które będą odpowiadać akceptowalnemu poziomowi. Oto kilka przykładów:

* Stosowanie szyfrowania

* „Anonimowe" technologie routingu P2P, takie jak routing cebulowy (patrz rozdział 31 w tym podręczniku)

* Izolacja sieci dla komputerów używanych do uzyskiwania oprogramowania z aplikacjami P2P

* Połączenia z Internetem nabyte przez firmę za pomocą modemu DSL lub kablowego, co pozwala uniknąć korzystania z zasobów sieci firmowej

Odpowiedź.

Wszystkie organizacje muszą dokładnie określić, w jaki sposób reagować na naruszenia bezpieczeństwa i naruszenia zasad, w tym sytuacje, w których zaangażowana jest technologia P2P. Nie tylko proces ten powinien być uwzględniony w ogólnym planie bezpieczeństwa, ale także powinny istnieć procesy reagowania na incydenty w celu usunięcia z sieci systemów obraźliwych. W niektórych przypadkach odbudowa zagrożonego zasobu może być konieczne, ale niektóre organizacje mogą zdecydować się na usunięcie zhakowanej maszyny z produkcji i/lub zachowanie kopii maszyny do badań kryminalistycznych do celów prawnych, kryminalistycznych lub dochodzeniowych.

Studium przypadku.

Błędna konfiguracja, niezamierzone użycie, ciekawość i eksperymentowanie z P2P w miejscu pracy zdarzają się z konsekwencjami. Chociaż ten przypadek jest tylko jednym rodzajem konkretnego incydentu bezpieczeństwa związanego z technologią P2P, powinien służyć jako przykład tego, jak taka sytuacja może wystąpić. Pracownik jednej organizacji zgłosił do helpdesku wolno działający komputer. Wszystkie zwykłe sugestie i sztuczki helpdesk zostały wyczerpane z niewielkim wpływem na wydajność komputera. Występowały typowe objawy powolnego komputera — długi czas oczekiwania na wykonanie prostych zadań, przypadkowe błędy i wyłączenia, blokady i inne problemy operacyjne. Była jednak jedna różnica: po ponownym uruchomieniu komputer musiałby zwolnić i przestać odpowiadać przez kilka minut. Po pewnym czasie pracownik skomentował: „Próbowałem zainstalować program do udostępniania muzyki w zeszłym tygodniu, ale mi się nie podobał i odinstalowałem go". To skłoniło inżyniera do zbadania każdego procesu uruchomionego na komputerze. Chociaż wydawało się, że aplikacja P2P została odinstalowana, w rzeczywistości tak nie było; nadal był zainstalowany i działał w trybie ukrycia. Deinstalator maskował jedynie aplikację P2P. Nie tylko aplikacja P2P nadal działała, ale była źle skonfigurowana, aby udostępniać całą zawartość dysku C:. Do maszyny podłączonych było dosłownie tysiące innych użytkowników P2P aktywnie wyszukujących, przesyłających, pobierających i zmieniających zawartość dysku twardego komputera. Komputer nie tylko udostępniał wszystkie swoje dane, ale był używany jako serwer do obsługi tysięcy plików multimedialnych. Ponieważ komputer znajdował się w segmencie sieci, który miał pełną translację adresów sieciowych TCP/IP 1-do-1, był w rzeczywistości całkowicie otwarty na świat zewnętrzny - a świat zewnętrzny w pełni wykorzystywał tę

okazję. Dysk twardy był praktycznie pełny, a zdalni użytkownicy dodawali i usuwali pliki do woli. Zapora sieciowa hosta została nawet zmodyfikowana przez instalację aplikacji P2P, aby otworzyć wszystkie niezbędne porty dla świata. Nie wiadomo, czy do danych osobowych użytkownika rzeczywiście uzyskano dostęp, pobrano je lub wykorzystano do jakiejkolwiek złośliwej aktywności, ale z pewnością istniała taka możliwość. Z powodu nieautoryzowanego pobierania przez użytkownika, niewystarczającego bezpieczeństwa sieci i innych naruszeń zasad organizacja nie mogła być pewna poufności lub integralności komputera lub jego danych. Podjęto niezbędne kroki, aby zapobiec ponownemu wystąpieniu tego incydentu, ale ten scenariusz rozegrał się w innych organizacjach i będzie się powtarzał, dopóki istnieje ryzyko P2P.

ZABEZPIECZENIE NATYCHMIASTOWEJ WIADOMOŚCI.

Wiadomości błyskawiczne stały się integralną częścią komunikacji — zarówno biznesowej, jak i osobistej — dla wielu osób. W niedawnej przeszłości dość łatwo było po prostu stworzyć politykę, która zakazywała korzystania z komunikatorów internetowych do użytku osobistego i zezwalała tylko na wewnętrzne, biznesowe komunikaty w firmie. Jednak komunikatory internetowe stały się integralną częścią życia. Komunikatory internetowe są wszechobecne w większości organizacji — do użytku osobistego i biznesowego. W rezultacie, od kadry kierowniczej po stażystów, komunikatory internetowe można znaleźć na wielu komputerach, ale muszą być zarządzane i zabezpieczone na wszystkich.

Zagrożenia dla Firmy.

W przypadku każdej technologii, szczególnie tej, która łączy się z Internetem, istnieje ryzyko dla organizacji. Wiadomości błyskawiczne nie są drobną irytacją, którą należy lekceważyć; jeśli technologia nie jest kontrolowana przez organizację, może wystąpić poważne naruszenie bezpieczeństwa. Pamiętaj, że dzisiejsze komunikatory internetowe znacznie wykraczają poza sam txt; są w stanie przekazać znacznie więcej niż tylko przypadkowe, interpersonalne przekomarzanie się.

Utrata informacji.

Utrata informacji i utrata poufności, celowo lub nieumyślnie, są najprawdopodobniej największym zagrożeniem dla IM dla biznesu. Istnieje kilka sposobów szkodliwego przekazywania informacji za pośrednictwem IM8:

* Ujawnianie sekretów za pośrednictwem czatu tekstowego, zwłaszcza gdy firma podjęła duży wysiłek w celu filtrowania i blokowania takiej komunikacji za pośrednictwem poczty e-mail z bramami e-mail, zarządzaniem danymi własności intelektualnej i innymi technologiami

* Funkcje kopiowania i wklejania (w tym zrzuty ekranu) używane do przesyłania poufnych lub tajnych informacji z innych zabezpieczonych aplikacji lub środowisk

* Transfery plików

* Udostępnianie ekranu i funkcje współpracy w czasie rzeczywistym, takie jak współdzielone tablice lub funkcje udostępniania pulpitu

* Zapominanie o wyłączeniu sesji głosowej lub wideo i niezamierzonym przekazywaniu dźwięku lub obrazów do oryginalnego korespondenta - szczególnie niebezpieczne, gdy zostawiasz pocztę głosową przez klienta komunikatora

* Przekazywanie głosu, wideo lub obu stron innej stronie (niezamierzone lub celowe)

* Wykorzystanie technologii kamery internetowej do przekazywania informacji wizualnych w bezpiecznym obiekcie

* Pobieranie złośliwego oprogramowania w celu zbierania i kradzieży danych

* Podszywanie się (ta taktyka zwykle polega na kradzieży znanego konta IM lub stworzeniu fałszywego konta w celu podszywania się pod kogoś, kogo zna ofiara).

* Wezwania do sądu lub nakazy przeszukania wykonywane w celu zebrania dzienników komunikatorów, rozmów itp.

Chociaż nie jest to pełna lista, powinna służyć jako pomoc w planowaniu bezpieczeństwa i rozwoju polityki. Istnieje wiele dobrych zasobów w Internecie, w których można dokładniej wyjaśnić podobne zagrożenia i konsekwencje, ale powyższa lista powinna zachęcić do przemyślanej burzy mózgów na temat sposobów, w jakie organizacja może utracić dane. Niektóre wymienione metody byłyby niezwykle trudne do wykrycia i naprawienia. Dzięki szybkim sieciom i szybkim łączom internetowym w większości organizacji można przesłać ogromną ilość danych w krótkim czasie.

Konsekwencje.

Podobnie jak w przypadku innych zagrożeń bezpieczeństwa, konsekwencje niezabezpieczenia technologii IM mogą być poważne. Wiele współczesnych organizacji doświadczyło naruszenia bezpieczeństwa związanego z komunikatorami internetowymi, a prawdopodobnie będzie ich więcej. Naruszenia bezpieczeństwa wiadomości błyskawicznych mogą być śmiertelne dla organizacji same w sobie lub jako część znacznie większego ataku na firmę. Kradzież lub przesyłanie informacji za pośrednictwem komunikatorów internetowych jest nie mniej ryzykowne niż jakakolwiek inna forma kradzieży informacji. Pojedynczy plik, niezależnie od tego, czy został przesłany za pośrednictwem komunikatora internetowego, czy skrupulatnie wycięty i wklejony, krok po kroku przez długi czas, może zniszczyć reputację firmy i pozycję w oczach opinii publicznej, a nawet przynieść korzyści konkurencji. Włamanie z jednej rozmowy przez komunikator internetowy może potencjalnie obniżyć cenę akcji korporacji w ciągu kilku godzin lub dni. Zdarzały się nawet przypadki, gdy poufne informacje dyrektora generalnego zostały przechwycone i opublikowane w Internecie, aby wszyscy mogli je zobaczyć

Odmowa usługi.

Komunikator nie może być spisany na straty jako maleńka aplikacja bez rzeczywistego wpływu na zasoby sieciowe. Wiadomości błyskawiczne mogą być narzędziem wykorzystywanym do tworzenia ataku typu „odmowa usługi" na organizację, skutkującego utratą dostępności. Technologia IM może być dla napastnika potężnym i użytecznym narzędziem, w tym korzystaniem z klientów IM z bezpośrednim połączeniem z Internetem. Z odpowiednią kombinacją złośliwego oprogramowania i dostępu, atakujący może wykorzystać jedną z wielu luk wykrytych w aplikacjach IM, w tym stale popularne przepełnienie bufora.

Zapobieganie i łagodzenie.

Każda organizacja musi chronić się przed zagrożeniami powodowanymi przez technologię IM. W organizacji należy przeprowadzić właściwy przegląd i analizę ryzyka związanego z IM, a organizacja musi określić wielkość ryzyka, które jest gotowa podjąć. Konieczna jest również ocena kosztów i wysiłków związanych z zapobieganiem i łagodzeniem tego zagrożenia. Organizacje będą inaczej oceniać ryzyko i korzyści związane z korzystaniem z komunikatorów internetowych. Nie ma ustalonego standardu dla każdej organizacji lub firmy; nie ma uniwersalnego zestawu reguł, które można

zastosować we wszystkich sytuacjach. Następne sekcje zawierają strategie, taktyki i uwagi dotyczące zabezpieczania wiadomości błyskawicznych.

Polityka.

Polityka musi być na pierwszym miejscu, zwłaszcza przy popularności i powszechnym korzystaniu z komunikatorów internetowych. Bez odpowiednich zasad organizacja nie ma szans na rzeczywistą ochronę. Polityka musi być podstawą, na której opierają się wszystkie inne rozważania. Jasno zdefiniowana, dobrze skomunikowana i jednakowo egzekwowana polityka jest jedną z najważniejszych podstaw, na których opiera się bezpieczeństwo informacji. Bez względu na to, co organizacja zdecyduje, jeśli chodzi o zasady dotyczące komunikatorów internetowych, musi to być określone w polityce. Wiadomości błyskawiczne, choć ryzykowne, to jedna z najbardziej widocznych decyzji politycznych, jakie firma podejmie dla pracowników. Chociaż najlepszym rozwiązaniem i preferowanym ze względów bezpieczeństwa może być całkowite odrzucenie wiadomości błyskawicznych, co może prowadzić do sfrustrowanych pracowników, którzy nie będą mogli korzystać z obiektu do użytku osobistego, biznesowego lub obu. Każdy zespół zarządzający powinien być świadomy potencjalnych konsekwencji zbyt surowej polityki. Z drugiej strony, umożliwienie nieograniczonego dostępu do komunikatorów internetowych z pewnością nie jest najlepszym rozwiązaniem. Niektóre organizacje, w zależności od platformy oprogramowania, mogą być w stanie zapewnić pracownikom zarządzane środowisko wiadomości błyskawicznych, w którym pracownik może połączyć się z oficjalną platformą wiadomości błyskawicznych organizacji, a także z niektórymi popularnymi usługami wiadomości błyskawicznymi używanymi do komunikacji osobistej. Jednocześnie organizacja może centralnie wdrażać ustawienia, takie jak dozwolone usługi, sposób ich łączenia (szyfrowane lub nie) oraz używane opcje rejestrowania, w tym możliwość nagrywania lub archiwizowania rozmów. Należy wziąć pod uwagę zgodność i przepisy rządowe. Jeśli komunikacja z komunikatorami ma być dozwolona, może stać się częścią komunikacji biznesowej organizacji, a zatem może podlegać wezwaniu sądowemu, żądaniom otwartej dokumentacji oraz wymogom archiwizacji i przechowywania dokumentów. Może to być szczególnie niebezpieczne, jeśli wybrana platforma IM jest zintegrowana z systemem Voice over IP organizacji. Nowe regulacje i przepisy prawne mogą mieć duży wpływ na decyzje polityczne. Należy pamiętać, że dzienniki wiadomości błyskawicznych i konwersacje mogą być przedmiotem legalnego odkrycia, przeszukania i zajęcia. Skonsultuj się z radcą prawnym w celu uzyskania odpowiedniej porady prawnej.

Skutki całkowitego zakazu.

Zakaz wszystkich technologii komunikatorów internetowych byłby najlepszym sposobem na zapewnienie większego bezpieczeństwa przedsiębiorstwa. Spowoduje to jednak tylko niezadowolonych użytkowników, ale nie będzie skuteczne. Użytkownicy mogą szybko zaznajomić się z technologią, jeśli zdecydują się obejść zasady. Blokada komunikacji IM często powoduje, że użytkownicy robią prawie wszystko, co mogą, aby osiągnąć swój cel, jakim jest niezakłócony IM. Niektórzy klienci są projektowani z myślą o tym i z radością będą tunelować z powszechnie dozwolonych portów TCP/IP, takich jak 80, zwykle otwartych dla komunikacji HTTP. Oprogramowanie można skonfigurować tak, aby omijać reguły zapory, wykrywać i odwracać technologię kształtowania pakietów oraz tunelować jego drogę do Internetu za pomocą połączeń szyfrowanych. Wiele usług komunikatorów internetowych udostępnia również interfejsy wyłącznie internetowe, które nie wymagają instalowania oprogramowania podczas komunikacji za pośrednictwem protokołu HTTP. Niestety, ta technologia może być trudna i frustrująca do zakazania w organizacji; całkowity zakaz prawdopodobnie nie jest praktycznym rozwiązaniem.

Zapobieganie instalacji oprogramowania do obsługi wiadomości błyskawicznych.

Chociaż całkowity zakaz może nie być możliwy, a nawet pożądany, jednym z kroków, które może podjąć bezpieczniejsza organizacja, jest uniemożliwienie użytkownikom instalowania oprogramowania do komunikatorów internetowych. Ta taktyka nie rozwiąże całego problemu, ale z pewnością pomoże. Kontrolowanie instalacji oprogramowania do komunikatorów internetowych powinno być częścią ogólnej polityki instalacji oprogramowania w organizacji. Ogólnie rzecz biorąc, instalowanie oprogramowania bez pozwolenia powinno być zabronione. Jeśli jest to wykonalne, większości pracowników należy odmówić praw administratora lokalnej stacji roboczej. W wielu rozwiązaniach do zarządzania użytkownikami lub systemami możliwe jest również zablokowanie instalacji oprogramowania za pomocą szablonów i procedur polityk indywidualnych, grupowych lub stacji roboczych. Uniwersalne zapobieganie instalacji oprogramowania jest znacznie łatwiejsze niż próba zdefiniowania zasad lub szablonów dla każdego możliwego partnera, aplikacji, grupy lub narzędzia komunikatora internetowego.

Walcz z technologią za pomocą technologii.

Sama technologia nie zapewni organizacji kompleksowego rozwiązania do zabezpieczania wiadomości błyskawicznych. Istnieje jednak wiele urządzeń sieciowych, urządzeń, oprogramowania do monitorowania ruchu i innych technologii, które pomagają organizacji zminimalizować wykorzystanie komunikatorów internetowych. Nie wierz w twierdzenia marketingowe, że jakiekolwiek urządzenie lub technologia może gwarantować blokowanie komunikatorów; niewielu może dotrzymać tej obietnicy. Jedynym prawdziwym sposobem na zagwarantowanie firmy wolnej od komunikatorów internetowych jest całkowite zablokowanie dostępu do Internetu, co nie jest realistyczne. Organizacja może również wykorzystać istniejącą infrastrukturę bezpieczeństwa, taką jak IDS lub IPS.

Ogranicz ryzyko i narażenie.

W przypadku większości organizacji ograniczanie komunikatorów za pomocą zasad i technologii jest rozwiązaniem na zagrożenia, jakie wprowadza komunikator. Połączenie tych dwóch podejść pomoże zmniejszyć możliwość utraty danych. Menadżerowie ds. Bezpieczeństwa i administratorzy powinni uzgodnić, co można reklamować, czego nie wolno w organizacji. Organizacja może zdecydować się na zablokowanie przesyłania plików, funkcji kamery internetowej lub funkcji udostępniania ekranu w przypadku komunikacji za pomocą wiadomości błyskawicznych. Tego typu działania nie zapobiegną naruszeniom bezpieczeństwa komunikatorów, ale mogą ograniczyć utratę danych. Podobnie jak w przypadku każdej polityki i zarządzania ryzykiem, należy wprowadzić odpowiedni audyt, raportowanie i kontrole zgodności.

Zapewnianie bezpiecznych wiadomości błyskawicznych.

W środowiskach, w których komunikatory internetowe są potrzebne do prowadzenia działalności, najlepszą strategią jest zapewnienie pracownikom bezpiecznych, zarządzanych usług komunikatorów internetowych. Oczywiście potrzeby w różnych organizacjach będą się różnić w zależności od poziomu łączności, funkcji i oprogramowania IM. Wiele popularnych obecnie korporacyjnych systemów poczty e-mail i współpracy ma wbudowane lub opcjonalne usługi wiadomości błyskawicznych. Po prawidłowym wdrożeniu te systemy IM mogą spełniać wiele z tych najlepszych praktyk dotyczących bezpieczeństwa IM:

* Szyfruj komunikację IM tam, gdzie to możliwe: klient do serwera, serwer do Internetu i tak dalej.

* Szyfruj logi i rozmowy na czacie na stacji roboczej i serwerze.

* Upewnij się, że wszystkie dzienniki, rozmowy na czacie, przesyłanie plików i archiwa spełniają zasady dotyczące transmisji, przechowywania i niszczenia danych.

* Upewnij się, że funkcje „świadomości obecności” (funkcje oprogramowania, które pozwalają użytkownikowi komunikować swoją obecność lub dostępność, takie jak „online”, „poza domem” lub „na lunch” wszystkim użytkownikom) są zgodne z firmową polityką personalną.

* Administracyjnie wyłącz funkcje, których nie można zaszyfrować lub którymi nie można właściwie zarządzać (udostępnianie ekranu, przesyłanie plików, tablica itp.).

* Jeśli to możliwe, zablokuj lub wymuś ustawienia konfiguracji, aby zapewnić zgodność z zasadami.

* Ustanowienie procedur okresowego monitorowania i audytu systemów IM; nie ignoruj dzienników.

* Egzekwuj ostrożne zasady dotyczące haseł w systemach komunikatorów internetowych.

* Właściwie zabezpieczone systemy komunikacji IM z łącznością z Internetem; rozważ użycie serwerów proxy lub bram pośredniczących, które chronią wewnętrzne korporacyjne systemy komunikatorów internetowych; zapewnić odpowiednie zasady i procedury blokowania serwerów.

Systemy IM należące do firmy i zarządzane przez firmę mogą nie być możliwe we wszystkich sytuacjach. W takich przypadkach organizacja musi opracować zasady i procedury ograniczające ryzyko i narażenie w komercyjnych systemach komunikatorów internetowych. Niektóre systemy zapewniają „bezpieczne” wiadomości błyskawiczne, ale należy być sceptycznym co do dokładnej ochrony, jaką zapewniają. Rozważ ograniczenie komercyjnych potrzeb dotyczących wiadomości błyskawicznych do nieistotnych komputerów z ograniczonym dostępem do sieci, ograniczenie lub ograniczenie użytkowników do określonych aplikacji lub usług wiadomości błyskawicznych oraz monitorowanie ruchu sieciowego i wykorzystania wiadomości błyskawicznych. Niektóre komercyjne usługi IM oferują również usługi IM „korporacyjne” lub „biznesowe”, często za opłatą. Te oferty premium mogą zapewnić organizacji niezbędny lub akceptowalny poziom funkcjonalności i bezpieczeństwa. Dostęp do publicznych usług wiadomości błyskawicznych powinien być również zawsze blokowany z komputerów z uprzywilejowanym dostępem do krytycznych zasobów danych.

Odpowiedź.

Naruszenia wiadomości błyskawicznych i zhakowane systemy zazwyczaj nie wymagają specjalnej obsługi po incydencie związanym z bezpieczeństwem. Ogólnie rzecz biorąc, można postępować zgodnie z normalnymi zasadami i procedurami, aby właściwie badać, dokumentować i reagować na naruszenia bezpieczeństwa. Istnieje wiele narzędzi komercyjnych, w tym oprogramowanie śledcze, które pomagają w reagowaniu na incydenty. Zainfekowane lub zhakowane systemy, jeśli nie są już potrzebne do dochodzenia, powinny zostać ponownie zobrazowane przed przeniesieniem do pracownika; nigdy nie pozwalaj, aby maszyna została „oczyszczona” po awarii i przywrócona do produkcji.

Bezpieczne przesyłanie wiadomości.

Chociaż większość użytkowników w organizacji jest ogólnie zadowolona z głównych systemów, klientów i usług komunikatorów internetowych, istnieją zagrożenia, które należy wziąć pod uwagę. Wydaje się, że istnieje prawie nieograniczona liczba klientów komunikatorów typu open source, internetowych dostawców komunikatorów i czatów, serwisów społecznościowych oferujących komunikatory internetowe i tym podobnych. Rozważając politykę i zarządzanie komunikatorami internetowymi w organizacji, ważne jest, aby przeanalizować źródło i intencje wszystkich możliwych usług. Całe oprogramowanie i usługi komunikatorów internetowych nie są sobie równe; niektóre mogą pochodzić z niezaufanych źródeł i mogą zawierać złośliwe oprogramowanie i inne zagrożenia bezpieczeństwa, takie jak złodzieje haseł lub keyloggery. Oprogramowanie do obsługi wiadomości

błyskawicznych lub dostawcy mogą również zdalnie rejestrować informacje bez wiedzy lub zgody użytkownika. Ponadto, jeśli organizacja będzie korzystać z komercyjnego oprogramowania i usług komunikatorów internetowych, bardzo ważne jest dokładne zapoznanie się z warunkami użytkowania i umowami licencyjnymi dostawcy. Obowiązki i zobowiązania obu stron powinny być dokładnie rozważone przez menedżerów ds. bezpieczeństwa informacji, kierownictwo firmy i radcę prawnego przed zezwoleniem na korzystanie z oprogramowania i powiązanych usług.

ZABEZPIECZENIE SMS.

Niewiele technologii jest bardziej wszechobecnych niż SMS. Praktycznie wszystkie telefony komórkowe są zdolne do wysyłania i odbierania wiadomości SMS. Ponieważ telefony komórkowe są praktycznie wszędzie, należy uwzględnić względy bezpieczeństwa, aby chronić się przed zagrożeniami, które ze sobą niosą. Technologia o stosunkowo niewielkim śladzie może spowodować zniszczenie świata, gdy zostanie użyta jako broń. Obecnie technologia SMS i związane z nią usługi uzupełniające rozwijają się wykładniczo. Zabezpieczenie i obrona przed SMS-ami muszą być uwzględnione w kompleksowym planie bezpieczeństwa każdej organizacji. Aby zrozumieć bezpieczeństwo SMS-ów, ważne jest również wyjście poza telefon komórkowy. Aby korzystać z tej technologii, SMS nie wymaga telefonu komórkowego. Wielu operatorów telefonicznych pozwala na generowanie i wysyłanie wiadomości SMS z niezabezpieczonej, publicznej strony internetowej. Wiadomości SMS mogą również pochodzić z wiadomości e-mail, usług wiadomości błyskawicznych i tym podobnych. Wiadomości SMS mogą nawet pochodzić z usług subskrypcyjnych, takich jak dzienny horoskop lub krytycznych systemów, takich jak usługi powiadamiania awaryjnego. Poza tym dzisiejsze telefony komórkowe, w tym smartfony, są bardziej wydajne i zawierają o wiele więcej funkcji i nie wykazują oznak spowolnienia. Telefony zyskują coraz większą moc obliczeniową, pamięć, złożone systemy operacyjne i inne funkcje, które zasadniczo mogą na nowo zdefiniować urządzenie jako komputer osobisty. Telefony mogą łączyć się z Internetem, instalować aplikacje, komunikować się z telefonu na telefon, a nawet uzyskiwać dostęp do firmowych sieci danych. Menedżerowie i specjaliści ds. bezpieczeństwa informacji nigdy nie powinni lekceważyć mocy i wszechstronności telefonu komórkowego. Stanowią zagrożenie dla całego bezpieczeństwa informacji organizacji.

Zagrożenia dla Biznesu.

SMS może wprowadzić do organizacji wiele rodzajów zagrożeń bezpieczeństwa. SMS-y mogą spowodować naruszenie danych przez niewinne błędy lub celowe ataki. Technologia ta może być wykorzystywana jako narzędzie przestępcze do celowej kradzieży informacji, wydobywania danych, wyłudzania informacji i oszukiwania. Może to być również kanał do nieumyślnej utraty danych. Konsekwencje utraty danych przez SMS są stosunkowo takie same, jak w przypadku każdego innego naruszenia danych: utrata zaufania do organizacji, utrata wizerunku, zły public relations, kary finansowe i tak dalej. Poważne lub nawet niewielkie naruszenie danych może wydawać się komunikatem światu, że organizacja nie ma obowiązującego kompleksowego planu bezpieczeństwa lub firma nie przestrzega takiego planu – niezależnie od tego, czy jest prawdziwy, czy nie. Niektórzy inwestorzy, klienci lub ludzie z całej społeczności mogą spojrzeć na naruszenie tak prostej technologii i zapytać: „Jak firma może nie mieć odpowiedniego zabezpieczenia dla czegoś tak prostego jak telefon komórkowy?” Brak laptopa z poufnymi danymi to poważne naruszenie bezpieczeństwa, ale telefon komórkowy, ze wszystkimi jego możliwościami, musi być traktowany jako prawie ten sam rodzaj krytycznego wykroczenia.

SMS jako narzędzie do celowej utraty danych.

Jednym z niebezpieczeństw, jakie może napotkać organizacja, jest osoba lub grupa osób wykorzystująca technologię SMS do przesyłania krytycznych danych do osób nieuprawnionych, zwykle

spoza organizacji. To działanie byłoby powieleniem starej taktyki kradzieży informacji kawałek po kawałku z wewnątrz organizacji komuś, kto nie powinien posiadać tych informacji. Rozważ klasyczne sztuczki przestępców, takie jak kopiowanie informacji w małych kawałkach przez długi czas, aby uniknąć podejrzeń. Do przenoszenia danych można użyć dowolnej liczby technologii, w tym pamięci flash lub pendrive'ów, iPodów, skrawków papieru, zdjęć, wydruków ekranowych, wbudowanego kodu, a nawet zapamiętywania. Niezadowoleni pracownicy mogą wysyłać SMS-y z poufnymi informacjami wspólnikowi lub nawet sobie w celu późniejszego wykorzystania, takiego jak sprzedaż danych, wymuszenie i tym podobne. Byłoby praktycznie niemożliwe, aby wiedzieć, że pracownik powoli wycieka dane poza firmę z telefonu komórkowego, zwłaszcza gdy ten telefon nie jest własnością organizacji ani nie jest przez nią kontrolowany. To, co może wydawać się współpracownikom poważnym uzależnieniem od wiadomości tekstowych, może w rzeczywistości być poważnym naruszeniem danych. Innym faktem, który zarządzanie bezpieczeństwem informacji musi wziąć pod uwagę, jest to, że usługa SMS, niezależnie od tego, czy jest dokładnie zgodna z pierwotną definicją, czy nie, rozszerzyła się znacznie poza wiadomości o długości zaledwie 160 znaków. Użytkownicy telefonów komórkowych mogą wysyłać strumienie wideo w czasie rzeczywistym, nagrane wideo, zdjęcia, znacznie dłuższe wiadomości tekstowe przekraczające 160 znaków, linki do stron internetowych i prawie wszystko, co operatorzy telefonii mogą wdrożyć. Jeśli branża telefonii komórkowej uważa, że wszystkie te funkcje są równoznaczne z SMS-em, plan bezpieczeństwa organizacji również powinien. Ryzyko biznesowe znacznie wzrosło z każdym dodaniem nowej technologii.

Nieumyślna utrata danych przez SMS.

Utrata danych może nastąpić w wyniku pomyłki, pecha, głupoty, błędnego poinformowania użytkownika lub niezrozumienia funkcji, a także kradzieży samego urządzenia z danymi. Zarówno celowa kradzież danych, jak i nieumyślna utrata danych są niezwykle niebezpieczne, z potencjalnie poważnymi konsekwencjami. Wyszukiwarki ujawniają wiele różnych taktyk i wojennych historii utraty danych z telefonu komórkowego, a także inne problemy bezpieczeństwa związane z SMS-ami. Oto scenariusze i techniki do rozważenia:

* SMS przez e-mail lub Internet

* Podsłuchiwanie lub podsłuchiwanie SMS-ów

* Odzyskiwanie niewłaściwie usuniętych danych

* Skradzione, pomieszane lub zgubione telefony

* Błędne numery

* Łączność Wi-Fi

* Telefon bez nadzoru bez hasła

* Złośliwe oprogramowanie zainstalowane na telefonie (keyloggery)

* Telefon odbiorcy został zgubiony, skradziony lub pożyczony

* Podszywanie się

Zapobieganie i łagodzenie.

Technologia SMS nie zniknie w najbliższym czasie, dlatego każda organizacja musi opracować plan zapobiegania utracie danych i ochrony przed tym ryzykiem. Po raz kolejny kierownictwo organizacji, zarządzanie bezpieczeństwem i specjaliści ds. bezpieczeństwa muszą ocenić ryzyko związane z SMS w

porównaniu z potrzebą prowadzenia działalności i utrzymania przyjaznej grupy pracowników. Każda organizacja musi sama zdecydować, jakie dokładnie praktyki zastosować w celu zapewnienia bezpieczeństwa SMS-ów oraz jakie są koszty/korzyści z każdej praktyki. Należy wziąć pod uwagę wszystko, od zasad i procedur, po wdrażanie technologii bezpieczeństwa i usług świadczonych przez firmy zajmujące się telefonią komórkową. Przy dzisiejszych zmieniających się potrzebach, nowo pojawiających się technologiach i szerokiej gamie telefonów komórkowych, dwóm organizacjom trudno jest zastosować tę samą ochronę i strategie łagodzenia. Jednak kolejne sugestie mogą być wykorzystane do rozpoczęcia, aktualizacji lub ulepszenia planu bezpieczeństwa organizacji w przypadku technologii SMS.

Polityka.

Należy opracować politykę SMS dla wszystkich telefonów komórkowych, które są własnością firmy lub są sponsorowane przez firmę. Polityka, gdy jest napisana na solidnych podstawach, jest kluczem do egzekwowania przez zasoby ludzkie, zwłaszcza gdy coś może skończyć się sporem sądowym. Niejasne zasady dopuszczalnego użytkowania nie wystarczą. Jasno określone stanowisko musi być spisane, przyjęte i przekazane wszystkim pracownikom. Polityka powinna mieć zastosowanie do każdego pracownika, kierownika lub stażysty, bez wyjątków. Polityka powinna być regularnie przeglądana, aktualizowana i redystrybuowana, w razie potrzeby z okresowymi szkoleniami, zwłaszcza w szybko zmieniającym się świecie, takim jak technologia mobilna. Dobra polityka musi również uwzględniać ważne rozróżnienie wspólne dla korzystania z telefonów komórkowych w organizacji: telefony osobiste a telefony firmowe/sponsorowane. Polityka musi określać: jakie zachowanie pracownika jest dopuszczalne w pracy; czy na terenie obiektu dozwolone są telefony osobiste; jaki rodzaj telefonu jest dozwolony (zazwyczaj odnosi się do tego, czy pracownicy mogą mieć smartfony); gdzie, kiedy i w jakich celach mogą używać osobistych telefonów komórkowych; co jest dozwolone w telefonach firmowych; i tym podobne.

Zakaz telefonu komórkowego.

W niektórych przypadkach potrzeby bezpieczeństwa mogą wymagać zakazu używania lub nawet posiadania telefonów komórkowych na terenie firmy lub w niektórych obszarach. Tego typu działania powinny być uwzględnione w polityce firmy i powinny być jasno zakomunikowane. Konieczne może być również przypominanie pracownikom za pomocą znaków i powtarzającej się komunikacji. Jest to powszechna praktyka zapobiegania utracie danych z dowolnej funkcji telefonu komórkowego, w tym SMS-ów. Organizacja powinna wprowadzić rozróżnienie na telefony należące do pracowników i sytuacje awaryjne. Jeśli obszar wymaga wysokiego poziomu bezpieczeństwa, zachowaj ostrożność i całkowicie zabroń używania telefonów komórkowych. Polityka musi obejmować odwiedzających, dostawców, wykonawców i inne podmioty zewnętrzne, jak również każdemu pracownikowi – bez względu na rangę.

Zapewnienie bezpiecznego SMS-a.

Dostarczenie „bezpiecznych” SMS-ów może okazać się trudne i łatwo popaść w fałszywe poczucie bezpieczeństwa. Menedżerowie ds. bezpieczeństwa informacji muszą dokładnie wiedzieć, jak działa ich infrastruktura telefonii komórkowej, zanim ogłoszą, że system jest bezpieczny. Chociaż jeden element połączenia telefonu może być bezpieczny — na przykład od telefonu do infrastruktury przesyłania wiadomości — cała ścieżka wiadomości SMS może nie być bezpieczna. Niektóre urządzenia, takie jak BlackBerry firmy Research in Motion, zapewniają szyfrowany transport wiadomości. Jednak wiadomości e-mail lub wiadomości do użytkowników w różnych sieciach telefonicznych lub na innych serwerach wiadomości mogą nie być szyfrowane. Specjaliści ds. bezpieczeństwa informacji muszą jasno rozumieć technologię, którą wdrażają, i muszą testować pod

kątem prawidłowej instalacji i konfiguracji, a także współpracować z dostawcą w celu weryfikacji oświadczeń marketingowych. Należy jednak pamiętać, że jeśli rozwiązanie nie jest tak bezpieczne, jak wymagają tego zasady i potrzeby organizacji, SMS-y, telefony komórkowe lub oba te elementy powinny zostać zakazane. Niektóre telefony lub rozwiązania dla smartfonów umożliwiają administratorom „blokowanie" usług, takich jak SMS, lub instalowanie oprogramowania do bezpiecznej komunikacji. Uważnie rozważ i oceń wszystkie opcje i rozwiązania.

Przynieś własne urządzenie.

Kiedyś standardem korporacyjnym był BlackBerry, dostarczany przez Research in Motion. Choć wciąż popularna i najłatwiejsza w zarządzaniu platforma dla smartfonów, w dzisiejszej organizacji pojawił się znacznie nowszy problem. Zmiany w prawie podatkowym sprawiły, że telefony komórkowe dostarczane przez firmę należą już do przeszłości. Dziś zasadą jest przyniesienie własnego urządzenia; coraz częściej jest to niezarządzany smartfon Apple iPhone lub Google Android. Pracownicy będą chcieli podłączyć swój smartfon do systemu poczty e-mail i kalendarza organizacji, a także korzystać z infrastruktury Wi-Fi. Będą chcieli pozostać w kontakcie z powodów zawodowych (firmowa poczta e-mail zapewnia im łączność z biurem i większą produktywność), łączyć się z powodów osobistych (osobista poczta e-mail, sieci społecznościowe) i korzystać z oszczędzającej baterię Wi-Fi zamiast komórkowych sieci danych. Z drugiej strony mogą chcieć użyć swojego telefonu do powiązania innego urządzenia bezprzewodowego przez Wi-Fi, gdzie nie mogą lub nie mogą łączyć się z firmową siecią Wi-Fi. To, w połączeniu z wiedzą, że te urządzenia są niezarządzane, mają prawie nieograniczoną liczbę nieznanych aplikacji lub „aplikacji" i zasadniczo są małymi komputerami mobilnymi, wystarczy, aby większość specjalistów ds. bezpieczeństwa skrzywiła się. Coraz trudniej jest powiedzieć pracownikom „nie", jeśli chodzi o korzystanie z tych urządzeń w miejscu pracy, zwłaszcza gdy czasami jest to wymagane w swojej pracy. To nowe wyzwanie musi zostać uwzględnione w polityce organizacji dotyczącej telefonów komórkowych/komputerów mobilnych. Powinno być ściśle określone, co jest dozwolone, a co nie i jak przepisy będą egzekwowane. Z funkcji zarządzania urządzeniami należy korzystać, jeśli pozwala na to platforma organizacji, aby kontrolować takie rzeczy, jak szyfrowanie, synchronizacja poczty e-mail, przechowywanie danych, hasła urządzeń i blokowanie urządzeń.

Inne względy.

Kolejna lista zawiera punkty, które należy wziąć pod uwagę podczas planowania bezpieczeństwa SMS-ów, z których wiele pochodzi ze specjalnej publikacji NIST 800-48 „Bezpieczeństwo sieci bezprzewodowej".

1. Stwórz zasady i procedury postępowania w przypadku zgubionych telefonów komórkowych. Telefon może zawierać wrażliwe dane, w tym zapisane i usunięte wiadomości SMS.

2. Jeśli telefony komórkowe są zakazane na terenie organizacji, upewnij się, że ochrona fizyczna posiada procedury i zasady sprawdzania telefonów komórkowych gości i pracowników.

3. Wiele telefonów komórkowych ma możliwość tworzenia kopii zapasowych i synchronizowania ich zawartości z pulpitem. Zapewnij odpowiednie procedury w celu zabezpieczenia danych i wycieku danych.

4. Powinny istnieć zasady i procedury ograniczające nabywanie telefonów komórkowych przez pracowników i zarządzanie nimi – pracownicy ochrony informacji mogą nie zdawać sobie sprawy z istnienia nowych telefonów w środowisku.

5. Telefony komórkowe nie są łatwe do audytu, nie ma też zbyt wiele oprogramowania wspomagającego proces audytu.

6. Pomimo prawidłowego oznakowania firmowego urządzenia, zgubione urządzenie rzadko będzie zwracane do organizacji. Zaplanuj złagodzenie szkód spowodowanych przez zgubiony telefon komórkowy; korzystać z funkcji bezpieczeństwa, takich jak zdalne czyszczenie urządzenia po utracie urządzenia za pomocą funkcji „zatrutej pigułki" lub funkcji „automatycznego niszczenia" po kilku próbach podania nieprawidłowego hasła.

7. Jeśli urządzenie mobilne obsługuje hasła blokady ekranu i włączania, używaj tych prostych zabezpieczeń, gdy tylko jest to możliwe.

8. Poprzez politykę i edukację zapobiegaj jak największej liczbie poufnych i prywatnych informacji na telefonach komórkowych organizacji, w tym wiadomości SMS.

9. W miarę możliwości wykorzystuj technologię infrastruktury klucza publicznego (PKI).

10. Jeśli to możliwe, zainstaluj oprogramowanie antywirusowe.

11. Wykorzystaj technologię VPN i firewall, aby zapewnić bezpieczniejszą transmisję danych.

12. Jeśli telefon ma być przewożony w podróżach międzynarodowych, wysyłanie SMS-ów powinno być zabronione, jeśli to możliwe. Ryzyko związane z zabieraniem telefonu komórkowego do międzynarodowych miejsc docelowych rośnie wykładniczo.

Reakcja i odpowiedź.

Gdy zdarzy się incydent bezpieczeństwa związany z telefonem komórkowym i SMS-em, chyba że organizacja posiada własny personel przeszkolony w zakresie reagowania na incydenty mobilne lub kryminalistyki, najlepiej będzie współpracować z operatorem telefonii komórkowej, być może również z producentem. Procedury i prawidłowe procesy związane z odzyskiwaniem, przechowywaniem, badaniem itp. danych najlepiej radzą sobie z najbardziej wykwalifikowanymi osobami. Jeśli to konieczne, zaangażuj organy ścigania. Jest to obszar, w którym długotrwałe dobre relacje z lokalnymi, stanowymi lub federalnymi organami ścigania są niezwykle korzystne – nawet jeśli dochodzenie niekoniecznie wymagałoby dochodzenia organów ścigania. Więcej informacji na ten temat znajduje się w rozdziale 61 niniejszego podręcznika. Badanie problemów związanych z SMS-ami, w tym śledzenie wiadomości, śledzenie lokalizacji telefonu i śledzenie ścieżki, jaką przebyła wiadomość SMS, można często przeprowadzić z pomocą operatora telefonii komórkowej. Egzekwowanie prawa i wezwania sądowe mogą być konieczne, w zależności od sytuacji. Zaatakowane urządzenia należy dokładnie sprawdzić przed przywróceniem ich do normalnego użytkowania. Dostawcy telefonii komórkowej mogą pomóc w „wyczyszczeniu" urządzenia z całego oprogramowania, w tym złośliwego oprogramowania, jeśli urządzenie nie ma takiej wbudowanej funkcji. Konkretne praktyki i procedury różnią się w zależności od telefonu i dostawcy, ale niektóre organizacje mogą również zdecydować się na archiwizację lub niszczenie urządzeń związanych z jakimkolwiek naruszeniem bezpieczeństwa. Systemy informacyjne, które zapewniają narzędzia do współpracy online, są coraz cenniejszymi narzędziami biznesowymi. Chociaż narzędzia te zapewniają doskonałe kanały do zwiększonej wymiany informacji, mają również potencjał do zwiększania zagrożeń bezpieczeństwa. Nawet sam Internet, z wieloma witrynami poświęconymi udostępnianiu informacji, oprogramowaniu do pracy grupowej, współdzielonym narzędziom i przechowywaniu danych, stał się obszarem współpracy. W planie bezpieczeństwa każdej organizacji należy uwzględnić nowe funkcje i ruchy, takie jak Google Apps, „Web 2.0", „Chmura", a nawet bezpłatne lub internetowe usługi połączeń konferencyjnych. Charakter współpracy i potrzeba efektywnego prowadzenia działalności biznesowej mają kluczowe znaczenie dla większości współczesnych organizacji. Wiele firm i organizacji stara się wykonać więcej pracy przy mniejszej liczbie osób. Technologia stała się ważnym partnerem umożliwiającym pracownikom

współpracę i osiąganie więcej w krótszym czasie. Narzędzia do współpracy stały się jeszcze bardziej istotne, gdy firmy rozszerzają się, obejmując współpracujących ze sobą ludzi z różnych lokalizacji geograficznych.

Bezpieczeństwo kontra otwartość.

Jedną z długotrwałych bitew o menedżerów ds. bezpieczeństwa jest bezpieczeństwo kontra otwartość lub funkcjonalność. Charakter współpracy wymaga nieograniczonego udostępniania danych i informacji, co może być trudne do zabezpieczenia. Organizacje muszą znaleźć odpowiednią równowagę między umożliwieniem użytkownikom swobodnej i otwartej wymiany informacji a zapewnieniem wymaganego poziomu bezpieczeństwa. Znalezienie tej równowagi wymaga współpracy i szacunku między dwiema grupami: tymi, którzy używają narzędzi i tymi, którzy są odpowiedzialni za zabezpieczenie organizacji. Obie grupy muszą w pełni zrozumieć swoje stanowisko; bez tego zrozumienia nie może dojść do znalezienia kompromisu i negocjacji kompromisu. Celem organizacji z pewnością musi być sprawny, nieprzerwany biznes, ale nie kosztem dobrego bezpieczeństwa. Jedynym sposobem na pokonanie tej komplikacji jest dobroduszna, otwarta i zorientowana na cel komunikacja. Nie jest to problem lub proces związany wyłącznie z technologią informacyjną. Znalezienie optymalnej równowagi między bezpieczeństwem a funkcjonalnością będzie wymagało współpracy wszystkich typów kierownictwa i personelu. Chociaż może to dotyczyć wszystkich dziedzin bezpieczeństwa informacji, dotyczy to zwłaszcza bezpieczeństwa narzędzi do współpracy. Bez tej ważnej równowagi narzędzia są zasadniczo bezwartościowe: zbyt bezpieczne i nie będą używane, zbyt otwarte, a firma może ponieść katastrofalną utratę danych i integralności. Niektóre firmy nie są w stanie się podnieść po takiej stracie.

Niebezpieczeństwa związane z narzędziami do współpracy.

Narzędzia do współpracy stają się potężne i muszą mieć pełne względy bezpieczeństwa. Nie należy instalować tych narzędzi, uzyskiwać do nich dostępu online ani integrować z firmą bez odpowiedniego planowania, analizy ryzyka, konfiguracji zabezpieczeń i testowania; Doraźne, niezarządzane systemy, instalowane bez wiedzy pracowników ochrony, muszą być zabronione, a naruszenia korygowane. Narzędzia do współpracy mogą łatwo stać się koszmarem dla zarządzania bezpieczeństwem, zwłaszcza jeśli zabezpieczenie tych narzędzi nie jest od samego początku kwestią priorytetową. Projektowanie i wdrażanie środków bezpieczeństwa w już wdrożonym systemie produkcyjnym jest niezmiennie frustrującym i daremnym ćwiczeniem zarówno dla użytkowników, jak i personelu zajmującego się bezpieczeństwem informacji. Podobnie, odkrycie po fakcie, że narzędzie do współpracy oparte na chmurze stało się kluczowe dla organizacji, jest przerażającą myślą dla większości specjalistów ds. bezpieczeństwa. Niektóre funkcje i ogólne zagrożenia związane z wieloma z tych systemów obejmują utratę poufności, integralności lub dostępności. Te zagrożenia mogą wystąpić z powodu któregokolwiek z tych problemów:

* Brak wymagań dotyczących uwierzytelniania, zasad lub procedur. System szeroko otwarty lub ze słabym uwierzytelnianiem umożliwiłby dostęp osobom nieuprawnionym.

* Podsłuchiwanie lub przechwytywanie danych. Transmisja danych do iz systemu może zostać przechwycona przez nieznane osoby.

* Podszywanie się. Udowodnienie, kim jest użytkownik, może być trudne, jeśli nie jest dobrze zarządzane, zwłaszcza przy słabych metodach uwierzytelniania i autoryzacji.

* Nieautoryzowane publikowanie poufnych informacji w niezabezpieczonych lub publicznych miejscach.

* Błędna konfiguracja. Prosty błąd w konfiguracji może ujawnić prywatne informacje.

* Wyszukiwarki. Dokumenty lub inne informacje mogą być przedmiotem robotów/agentów/pająków wyszukiwarek, jeśli nie zostaną ustanowione odpowiednie zabezpieczenia.

* Nieuczciwe systemy współpracy. Jeśli dział lub grupa wdraża własne narzędzia, prywatnie lub publicznie, bez wiedzy grupy bezpieczeństwa, nie można zagwarantować odpowiedniego bezpieczeństwa.

* Zagrożenia wewnętrzne. Nie można zajmować się tylko zagrożeniami zewnętrznymi. System współpracy jednego działu może być nieograniczoną pokusą innego działu.

* Użytkownicy. Użytkownicy nie zawsze mają na uwadze bezpieczeństwo. Małe błędy lub skróty mogą prowadzić do poważnych naruszeń bezpieczeństwa.

Podczas wdrażania lub oceny narzędzi do współpracy należy przeprowadzić analizę ryzyka w celu określenia, czy organizacja jest w stanie i chce zaakceptować związane z tym ryzyko. Grupy bezpieczeństwa powinny dokładnie przeprowadzić burzę mózgów i zbadać jak najwięcej możliwych zagrożeń bezpieczeństwa systemu współpracy. Korzystna może być współpraca z grupą wsparcia dostawcy rozwiązania w celu zminimalizowania lub wyeliminowania jak największej liczby zagrożeń bezpieczeństwa. Grupy robocze korzystające z narzędzi do współpracy pokładają duże zaufanie w aplikacji i narzędziach. Wiele z dostępnych obecnie aplikacji jest lekkich pod względem bezpieczeństwa i ciężkich cech rynkowych. Chociaż wiele firm internetowych poważnie podchodzi do kwestii bezpieczeństwa danych, nie są one właścicielami ani obrońcami danych organizacji; to nadal zależy od organizacji.

Zapobieganie i łagodzenie.

Narzędzia i systemy współpracy powinny być objęte taką samą dbałością o bezpieczeństwo, jak każdy inny system informatyczny. Chociaż charakter współpracy może być nieco otwarty, powinny obowiązywać te same zasady, procedury i staranne kontrole. Celem musi być nadal poufność, integralność i dostępność danych oraz systemu informacyjnego. Narzędzia do współpracy muszą nadal przynosić korzyści firmie, zapewniając jednocześnie, że firma nie ucierpi w wyniku incydentu związanego z bezpieczeństwem. Podejmując niezbędne kroki w celu zapobiegania problemom z zabezpieczeniami i łagodzenia ich skutków, narzędzia do współpracy mogą być nieocenione dla organizacji. Kolejne sugestie można wykorzystać, aby pomóc organizacji w zabezpieczeniu narzędzi i systemów współpracy.

Polityka.

Można się spierać, czy narzędzia współpracy wymagają określonych, oddzielnych zasad. Co ważniejsze, istnieje kompletna, dobrze napisana i dobrze skomunikowana polityka, zawierająca postanowienia dotyczące narzędzi współpracy, systemów i powiązanej technologii. Jasne zrozumienie i komunikacja w zakresie bezpieczeństwa narzędzi do współpracy muszą być dobrze zbadane, dobrze napisane, zwięzłe, dobrze komunikowane i regularnie aktualizowane. Niezwykle ważne jest, aby polityka pozostała aktualna, ponieważ opracowywane i wdrażane są nowe i bardziej złożone narzędzia współpracy. Zasady powinny również obejmować opcje bezpieczeństwa, które w innym przypadku mogą być poza kontrolą organizacji. Na przykład, jeśli firma zabrania korzystania z publicznych usług udostępniania plików, polityka powinna obejmować użytkowników próbujących korzystać z usługi spoza organizacji, jak również wewnątrz niej. Pracownicy nie powinni mieć możliwości korzystania z usług lub systemów, które nie są zgodne z zasadami, bez względu na to, gdzie iw jaki sposób usługa ma być używana. Dobra polityka powinna być inkluzywna, zwłaszcza jeśli dokładnie określa się, co

organizacja uważa za narzędzie współpracy. Łatwo byłoby zapomnieć o aplikacjach, takich jak poczta e-mail, komunikatory internetowe, spotkania online, blogi, sieci społecznościowe, współdzielone zasoby sieciowe, oprogramowanie do zdalnego dostępu, udostępnianie plików peer-to-peer i tym podobne. Wiele technologii zawiera komponenty współpracy, które należy wziąć pod uwagę, aby zapewnić bezpieczeństwo.

Uniemożliwić dostęp lub użycie.

Inną opcją, w połączeniu z polityką, jest zablokowanie korzystania z narzędzi do współpracy, w zależności od potrzeb organizacji. Może to obejmować wdrożenie technologii umożliwiającej osiągnięcie tego celu, w tym blokowanie treści, zapory ogniowe lub jedno i drugie. Powinno to uniemożliwić instalację lub używanie nieuczciwych narzędzi do współpracy. Należy przeprowadzać okresowe przeglądy systemów sieciowych i ruchu sieciowego, aby zapewnić zgodność z narzędziami do współpracy lub ograniczeniami.

Ogranicz dostęp.

Wiele narzędzi do współpracy można wdrożyć jako system tylko do użytku wewnętrznego, system oparty na chmurze lub oba. Organizacje będą chciały wybrać sposób, w jaki użytkownicy będą uzyskiwać dostęp do tych systemów. Na przykład uniemożliwienie niezabezpieczonej komunikacji z Internetu może pomóc w zwiększeniu bezpieczeństwa. Podobnie może być konieczne zablokowanie dostępu do usług publicznych z sieci organizacji. Lub rozwiązania techniczne, takie jak połączenia VPN spoza sieci organizacji, mogą zostać wykorzystane do zaspokojenia potrzeb komunikacyjnych.

Wdrażaj lub ulepszaj struktury i technologie zabezpieczeń.

Wszędzie, gdzie to możliwe, instaluj rozwiązania, które zwiększą bezpieczeństwo narzędzi do współpracy i które można zintegrować z istniejącymi strukturami bezpieczeństwa. Jeśli organizacja posiada rozwiązanie z pojedynczym logowaniem o wysokim poziomie bezpieczeństwa, zintegruj z nim systemy współpracy. Innym przykładem może być integracja systemów współpracy z nową lub istniejącą infrastrukturą PKI. Wykorzystaj dobrze znane i niezawodne rozwiązania, takie jak Secure Sockets Layer (SSL) i szyfrowanie dla hosta i wszystkich uczestników. To znacznie zmniejsza ryzyko naruszenia bezpieczeństwa podczas transmisji danych.

Audyt.

Bez względu na to, jaki poziom polityki, procedur lub środków zapobiegawczych zostanie wprowadzony, każda organizacja musi przeprowadzić audyt zgodności. Procedury audytu narzędzi współpracy i ich wykorzystania powinny być włączone do regularnych, ustrukturyzowanych funkcji audytu bezpieczeństwa informacji w organizacji. Wszelkie odstępstwa od zasad i procedur wymaganych dla narzędzi współpracy muszą być podejmowane w odpowiednim czasie.

Monitorowanie.

Każda organizacja, która wdraża narzędzia do współpracy, musi monitorować i raportować wykorzystanie systemu, wyniki audytu i zawartość danych. (Organizacja musi zbadać rzeczywistą zawartość danych, aby zapewnić zgodność z zabezpieczeniami, takimi jak chronione informacje zdrowotne [PHI] lub numer ubezpieczenia społecznego [SSN]. Z tego powodu wiele nowych produktów ma określone zasady). Monitorowanie i raportowanie działa w celu zapewnienia, że narzędzia współpracy a systemy są używane zgodnie z ich przeznaczeniem. Monitorowanie i raportowanie aktywnych projektów powinno szukać nietypowych wzorców użytkowania, naruszeń zasad, nieaktywnych użytkowników, nieaktywnych lub przestarzałych systemów i tym podobnych. Właściwe

zarządzanie systemem powinno już być wdrożone, ale ważne jest okresowe sprawdzanie systemów. Na przykład, jeśli grupa korzysta z systemu współpracy przy projekcie, po zakończeniu projektu wszystkie materiały projektowe i użytkownicy powinni zostać usunięci z systemu. Raporty z monitoringu i audytu systemu powinny być realizowane od razu.

Ostrożnie rozważ outsourcing i chmurę.

Niektóre organizacje są skłonne do korzystania z komercyjnych systemów współpracy wyłącznie online lub rozwiązań hostowanych. Nie należy podejmować tej decyzji pochopnie; rozważ ryzyko w porównaniu z zyskami. Organizacja powinna dokładnie przejrzeć wszystkie warunki świadczenia usług, umowy licencyjne, umowy dotyczące poziomu usług i obowiązki prawne. Aby zapewnić ochronę organizacji, należy zaangażować radcę prawnego, zwłaszcza w zakresie własności danych, ich posiadania, ustaleń prawnych i uprawnień do wezwania do sądu. Chmura ostatnio cieszy się dużym zainteresowaniem. Chociaż bezpieczeństwo chmury wykracza daleko poza zakres tego rozdziału, chmura nie powinna być traktowana inaczej niż jakakolwiek inna aplikacja zlecona na zewnątrz. Chmura często zawiera te same zagrożenia, co każda inna usługa, w której dane są przechowywane poza kontrolą organizacji. Bezpieczeństwo powinno być głównym problemem podczas oceny rozwiązań w chmurze, z uwzględnieniem:

* Umowy o poziomie usług

* Własność danych

* Technologia bezpieczeństwa danych używana podczas przechowywania danych (szyfrowanie, tworzenie kopii zapasowych, replikacja itp.)

* Odzyskiwanie danych, jeśli dostawca zostanie sprzedany, zamknięty lub zbankrutuje

* Fizyczna lokalizacja danych oraz jakie przepisy krajowe, stanowe lub lokalne mają zastosowanie do tej lokalizacji i danych

* Dostęp administratora (dla klienta i którzy administratorzy u usługodawcy również mają dostęp)

* Odpowiedzialność za bryczesy danych u usługodawcy

* Depozyt klucza dla zaszyfrowanych danych

Chociaż nie jest to wyczerpująca lista, powinna ona pomóc organizacji w burzy mózgów i badaniu zagrożeń związanych z narzędziami do współpracy w chmurze. Istnieje wiele zasobów online od renomowanych organizacji, które już dostarczyły wskazówek dla organizacji wchodzących w chmurę. Jak zwykle skonsultuj się z radcą prawnym.

Audyty i testy penetracyjne.

Podobnie jak w przypadku większości systemów informatycznych, zapewnienie niezbędnego bezpieczeństwa powinno obejmować regularne, zewnętrzne testy penetracyjne i audyty przeprowadzane przez osoby trzecie. Narzędzia do współpracy i powiązane systemy powinny być testowane i oceniane pod kątem ich sprawności w zakresie bezpieczeństwa. Wszelkie wykryte problemy powinny być udokumentowane i szybko naprawione. Pozwolenie neutralnemu, zewnętrznemu podmiotowi na niezależne testowanie systemu jest lepsze od testów wewnętrznych, dzięki czemu można wykluczyć stronniczość.

Aktualizuj narzędzia współpracy.

Niezwykle ważne jest aktualizowanie narzędzi do współpracy i powiązanych z nimi systemów informatycznych. Stosowanie łat na luki w zabezpieczeniach jest dobrą praktyką w zakresie technologii informatycznych i bezpieczeństwa informacji. Po dokładnym przetestowaniu poprawek w środowisku testowym, należy je jak najszybciej zastosować w środowiskach produkcyjnych. Nie ignoruj poprawek dostawców oprogramowania, zwłaszcza tych dotyczących znanych luk w zabezpieczeniach.

Reakcja i odpowiedź.

Po wykryciu naruszenia bezpieczeństwa związanego z narzędziami do współpracy należy postępować zgodnie ze zwykłymi zasadami i procedurami organizacji. Procedury dla skompromitowanych systemów informatycznych powinny być dobrze sformułowanymi, powtarzalnymi procesami w celu zachowania dowodów, zapewnienia szybkiego wykrywania i dochodzenia oraz spełniania niezbędnych wytycznych regulacyjnych. W razie potrzeby należy skorzystać z usług organów ścigania, doradców prawnych lub obu, aby zapewnić właściwe gromadzenie dowodów i dokumentację. Zasady powinny również dyktować procedury dotyczące zadań po zakończeniu dochodzenia, takich jak wymaganie kopiowania, archiwizowania, niszczenia, ponownego obrazowania lub ponownej instalacji zhakowanych systemów. Generalnie nie zaleca się próbowania po prostu „wyczyszczenia" zaatakowanego systemu. Zagwarantowanie, że zagrożony system ponownie będzie miał integralność, może być trudne.

WNIOSKI.

Przedstawiliśmy menedżerom i specjalistom ds. bezpieczeństwa zabezpieczanie technologię peer-to-peer, wiadomości błyskawiczne, usługi krótkich wiadomości i narzędzi współpracy. Sugestie i informacje mają pomóc w podejmowaniu decyzji dotyczących tych narzędzi w ramach ogólnego planu bezpieczeństwa organizacji. Wiele przykładów i koncepcji ma na celu pomoc w planowaniu, opracowywaniu polityki i przeglądzie ekspozycji organizacji na te technologie i związane z nimi zagrożenia. Powino służyć jedynie jako punkt wyjścia do badań organizacji na każdy temat i zapewnić, że menedżerowie ds. bezpieczeństwa informacji przynajmniej krótko rozumieją każdą koncepcję, związane z nią ryzyko, strategie zapobiegania i łagodzenia oraz sugestie reakcji. Trudno jest zarekomendować rozwiązania dla każdego rodzaju biznesu, dlatego każda organizacja musi dokonać własnego osądu w kwestii zabezpieczenia tych technologii. Popularność i wszechobecność narzędzi P2P, IM, SMS i współpracy zapewnia, że będą one częścią każdego planu bezpieczeństwa przez wiele lat.