WPROWADZENIE DO ZABEZPIECZENIA PRZECHOWYWANYCH DANYCH.

Omówimy metody zabezpieczania danych przechowywanych na nośnikach nieulotnych. Nośniki nieulotne obejmują dyski magnetyczne i ich (twarde) dyski, dyski kompaktowe (CD) i cyfrowe dyski wideo (DVD) z ich napędami optycznymi oraz dyski flash (znane również jako dyski USB, dyski flash i klucze pamięci). Ulotne urządzenia pamięci masowej, które nie są objęte tym rozdziałem, obejmują pamięć o dostępie swobodnym (RAM) i inną pamięć masową, która traci swoją zawartość w wyniku utraty mocy. Jedną z najważniejszych kwestii związanych z zarządzaniem bezpieczeństwem jest częsta utrata lub kradzież laptopów i innych mobilnych urządzeń komputerowych. Na przykład,

* Raport z 2008 roku sugerował, że w samych Stanach Zjednoczonych każdego roku na amerykańskich lotniskach pozostawia się ponad 600 000 laptopów, z czego około dwie trzecie pozostaje nieodebranych.

* W 2010 r. „…275 firm w Europie… straciło łącznie 72 000 laptopów, co kosztowało te organizacje łącznie 1,8 miliarda dolarów. Spośród 265 laptopów traconych przez przeciętną organizację rocznie firma zazwyczaj odzyskuje tylko 12”.

* W 2012 r. wskaźnik utraty wciąż wynosił 12 000 laptopów traconych tygodniowo na lotniskach w USA; innym szczegółem raportów z tamtych czasów było to, że nieodebrane laptopy były licytowane każdemu, kto był w stanie za nie zapłacić.

Nieszyfrowane pliki na tych skradzionych lub odkupionych laptopach stanowią zaproszenie do naruszenia poufności i kontroli. Na przykład audyt zużytych komputerów przeprowadzony przez rząd stanu New Jersey ujawnił, że „numery ubezpieczenia społecznego podatników, poufne raporty dotyczące wykorzystywania dzieci i przeglądy personelu pracowników z New Jersey prawie trafiły do oferenta, który zaoferował najwyższą cenę po tym, jak stan wysłał nadwyżki komputerów na aukcję ”. Ponadto „Prawie 80 procent wyrzuconych komputerów w próbce z biura kontrolera nie zostało oczyszczonych z danych przed wysłaniem do magazynu. ..” Od czasu ostatniego wydania tego podręcznika w 2008 r., głośne rozwiązania pamięci masowej są coraz częściej wykorzystywane przez osoby prywatne i organizacje, dlatego zawieramy krótkie omówienie bezpieczeństwa takich repozytoriów.

Podstawy zabezpieczeń dla administratorów pamięci masowej.

Systemy pamięci masowej rozwinęły się poza parasolem bezpieczeństwa innych zasobów organizacyjnych. Ponieważ obszar pamięci masowej jest jednym z najbardziej strategicznych elementów infrastruktury, profesjonaliści powinni z taką samą dbałością opracować kompleksowe mechanizmy kontroli bezpieczeństwa, jak te, które dotyczą pozostałej części sieci. Wielu dostawców skupiło się na rozwoju bezpiecznych środowisk pamięci masowej, które są skalowalne, ale elastyczne; większość dotyczy zarówno logicznych, jak i fizycznych aspektów bezpieczeństwa. Jednak każda odpowiednia strategia ochrony przechowywania danych zawiera równowagę między ochroną poufności i integralności informacji, a także zapewnieniem ich dostępności i użyteczności dla systemu i autoryzowanych użytkowników. Ostatecznie osoby odpowiedzialne za przechowywanie danych będą również miały za zadanie utrzymanie tej równowagi przy rozsądnych kosztach. Wiedza o tym, jak i gdzie dane będą przechowywane w sieci, oraz zajęcie się znanymi zagrożeniami dla danych jest najlepszą opcją, ponieważ często jest to bardziej efektywne pod względem wykorzystania zasobów (czasu i pieniędzy). Organizacja nie musi być głośnym podmiotem, aby cierpieć z powodu naruszonej puli danych. Pojedyncza kopia zapasowa może zawierać wystarczająco skoncentrowane informacje osobiste lub poufne informacje firmowe, aby doświadczyć utraty wiarygodności, utraty przychodów i

prawdopodobnie rzucenia organizacji na kolana. Co gorsza, kopia zapasowa, która jest nielegalnie kopiowana, może nie wykazywać oznak utraty kontroli nad poufnymi danymi.

Najlepsze praktyki

Każda organizacja musi dbać o sprawne działanie swoich aplikacji, serwerów i systemów użytkowników końcowych, aby móc korzystać z informacji oraz zachować najwyższy stopień dostępności i integralności informacji. Warstwowy model ochrony danych działa najlepiej; obejmuje warstwową obronę, należytą staranność i ograniczone zarządzanie. Wdrożone prawidłowo, bezpieczeństwo powinno być przejrzyste. Najlepsze praktyki w zakresie dostarczania bezpiecznego środowiska przechowywania danych obejmuje:

* Przeprowadzanie audytu i oceny ryzyka w infrastrukturze pamięci masowej w poszukiwaniu zagrożeń i słabych punktów.

* Wdrożenie uwierzytelniania w sieci pamięci masowej, które może koordynować autoryzację, konserwację haseł i szyfrowanie.

* Wdrażanie silnych kontroli dostępu opartych na rolach i przypisywanie praw dostępu stronom na podstawie wiedzy koniecznej.

* Przyjmowanie i egzekwowanie zasad szyfrowania i klasyfikacji danych. W oparciu o poziom klasyfikacji przypisany do danych, polityka organizacji może wymagać szyfrowania danych w spoczynku przez cały cykl życia danych. Mogą również istnieć wymagania dotyczące szyfrowania danych w locie (w całej sieci).

* Wymaganie silnych funkcji i praktyk bezpieczeństwa od dostawców systemów pamięci masowej i dostawców zewnętrznych pamięci masowych.

* Pamiętaj o zabezpieczeniu Storage Area Network (SAN) na poziomie przełącznika (lub sieci szkieletowej). Podział tkaniny na strefy to jedna z technik, która ogranicza dostęp do różnych części sieci SAN.

* Uwzględnienie wszelkich technologii replikacji danych lub replikacji magazynu w ogólnym planie bezpieczeństwa magazynu, w przypadku gdy taki ruch związany z replikacją może obejmować dzienniki transakcji i inne tymczasowe lokalizacje z częściowymi lub pełnymi kopiami danych wrażliwych.

* Ocena i wdrożenie zapobiegania utracie danych (DLP) do utrzymania bezpieczeństwa przechowywanych danych poza przedsiębiorstwem. Tagowanie danych lub etykietowanie wraz z dopasowywaniem wzorca (np. 999-99-9999 w przypadku numeru ubezpieczenia społecznego) są kluczem do pomocy w DLP.

* Tworzenie polityki usuwania starych urządzeń i nośników oraz usług przechowywania danych, w tym rutynowe wykonywanie zadań, takich jak bezpieczne czyszczenie lub fizyczne niszczenie wszystkich urządzeń i nośników przechowywania danych.

* Ocena i wdrażanie zasad przechowywania i niszczenia danych, zapewniając zgodność z wszelkimi obowiązującymi organizacyjnymi lub rządowymi kwestiami regulacyjnymi.

* Izolowanie sieci zarządzania pamięcią masową od podstawowej sieci organizacji. Nie izolując sieci, każdy pracownik potencjalnie ma dostęp do przechowywanych danych.

* Ustanowienie monitorowania dziennika dostępu.

* Przeprowadzanie kontroli pracowników i wykonawców w ramach procedur zatrudniania zasobów ludzkich (HR).

* Ustanowienie kontroli obiektów w organizacji w celu ograniczenia fizycznego dostępu do centrów danych, blokowanie szaf pamięci masowej i stojaków serwerowych, używanie zamków wbudowanych w niektóre serwery oraz zapewnienie niezawodności obwodu i budynku(ów) oraz weryfikacja, czy takie kontrole są stosowane dla zdalne lokalizacje przechowywania.

* Traktowanie bezpieczeństwa kopii zapasowych jako gwarantującego monitorowanie i alarmy o wysokim poziomie ważności. Przyjęcie zasad śledzenia i obsługi bezpiecznych nośników, które obejmują wymagania dotyczące tworzenia kopii zapasowych informacji finansowych, danych pracowników i własności intelektualnej.5 Rozdział 57 niniejszego podręcznika zawiera wiele informacji na temat tworzenia kopii zapasowych danych.

DAS, NAS i SAN

Istnieją trzy podstawowe metody przechowywania danych: magazyn bezpośrednio dołączany (DAS), magazyn sieciowy (NAS) i sieci magazynowania (SAN). Ponadto rośnie popularność zdalnego przechowywania danych z wykorzystaniem usług przetwarzania w chmurze, zwłaszcza wśród użytkowników indywidualnych, ale nawet organizacji. Dyski typu Direct Attached Storage to te, które są podłączone bezpośrednio do komputera. DAS może być albo wewnętrzny, umieszczony w obudowie komputera, albo zewnętrzny i podłączony przez połączenie elementów peryferyjnych, PCI, eSATA lub inny kanał magistrali. Zagrożeniem dla urządzeń DAS jest ich fizyczna kradzież lub dostęp za pośrednictwem obsługiwanego przez nie systemu komputerowego. Urządzenia Network Attached Storage to wyspecjalizowane serwery, na których działają zminimalizowane systemy operacyjne i systemy plików zaprojektowane specjalnie do obsługi wejścia/wyjścia (I/O) z innych serwerów. Serwery podłączone do urządzeń NAS mają DAS, który zawiera ich systemy operacyjne, aplikacje i inne komponenty, ale zwykle zapisują wszystkie dane na urządzeniu NAS przez połączenia TCP/IP przez Ethernet. NAS jest używany za pośrednictwem protokołu udostępniania plików, takiego jak Network File System (NFS) dla systemów UNIX i Server Message Block (SMB) lub Common Internet File System (CIFS) dla systemów Microsoft. (Ponieważ CIFS wyrósł z SMB, oba są często określane jako SMB/CIFS lub CIFS/SMB.) Podobnie jak w przypadku każdego połączenia Ethernet, połączenia między systemem a używanym przez niego serwerem NAS podlegają sniffowaniu, podsłuchiwaniu i do przechwytywania pakietów. Zagrożenia NFS i CIFS zostały omówione w dalszej części tego rozdziału. Sieci pamięci masowej to zbiory scentralizowanych dysków, do których można uzyskać dostęp z wielu serwerów. Korzystanie z sieci SAN może ułatwić rozwój firmy, ponieważ większość opcji sieci SAN umożliwia dodawanie dodatkowych dysków do puli w miarę wzrostu potrzeb w zakresie przechowywania danych, bez konieczności przełączania podłączonych systemów w tryb offline, co miałoby miejsce w przypadku dodawania nowego DAS do poszczególnych systemów. Tworzenie kopii zapasowych danych może być również łatwiejsze do kontrolowania, ponieważ potencjalnie można utworzyć kopię zapasową pojedynczego zasobu pamięci masowej zamiast każdego pojedynczego systemu. Dzięki wdrożeniu macierzy RAID lub innych implementacji redundancji dysków można zapisywać dane na wielu dyskach bez wpływu na wydajność serwerów aplikacji. Systemy można podłączać do sieci SAN różnymi metodami, w tym TCP/IP i kanałami światłowodowymi. Kanały światłowodowe omówiono w dalszej części tego rozdziału. Korzystanie z połączeń IP dla sieci SAN umożliwia serwerom łączenie się przez Internet, ale z tej opcji należy korzystać ostrożnie ze względu na obawy związane z bezpieczeństwem przesyłania danych przez Internet. Kopie zapasowe w chmurze wykorzystują łączność internetową do przechowywania danych kopii zapasowych w systemach zdalnych poza kontrolą właścicieli danych.

Zarządzanie przechowywaniem poza pasmem i wewnątrz pasma

Menedżerowie mogą być zmuszeni do zdalnego sterowania lokalizacjami magazynu, to znaczy z lokalizacji innej niż konsola podłączona bezpośrednio. Istnieją dwa podejścia do takiej komunikacji sterującej, z których każde wiąże się z własnymi problemami dotyczącymi bezpieczeństwa. Zarządzanie w paśmie wykorzystuje tę samą sieć, co transfery danych; Zarządzanie poza pasmem wykorzystuje oddzielną sieć. Podczas gdy zarządzanie pamięcią wewnątrzpasmową wykorzystuje te same kanały, które przechodzą dane w celu przechowywania, zarządzanie pozapasmowe wykorzystuje alternatywne metody. Na przykład rozwiązanie pozapasmowe może polegać na tym, że administrator pamięci masowej pracuje z biurka i łączy się z systemem pamięci masowej za pośrednictwem sieci podstawowej używanej przez wszystkich pracowników, podczas gdy dane przechodzą przez dedykowany kanał między serwerem aplikacji a systemem pamięci masowej. W przypadku zarządzania pozapasmowego należy rozważyć, w jaki sposób zapewnić, aby tylko autoryzowane systemy, takie jak administrator, łączyły się z systemem pamięci masowej. Jest to szczególnie konieczne, jeśli system pamięci masowej nie wymaga nawiązywania uwierzytelnionych połączeń przed zaakceptowaniem polecenia. Bez uwierzytelniania każdy system, który może komunikować się z systemem pamięci masowej, mógłby wydawać polecenia, które miałyby negatywny wpływ na system pamięci masowej. Inne ryzyko wiąże się z interfejsem używanym przez komunikację zarządzania i poleceniami przesyłanymi przez sieć bez szyfrowania. W przypadku systemów pamięci masowej, które są domyślnie zarządzane przez interfejsy HTTP, zamiast tego może być możliwe użycie protokołu HTTPS w celu ograniczenia ryzyka poleceń i logowania z przechwytywania pakietów sieciowych. Obawy budzi również zarządzanie wewnątrzpasmowe. Polecenia wysyłane w paśmie są zwykle wysyłane w postaci zwykłego tekstu. Inne zagrożenia związane z zarządzaniem pamięcią wewnątrzpasmową obejmują:

* Interfejsy zarządzania narażone na ataki typu „odmowa usługi” (DoS),

* Polecenia dostarczające informacji o innych urządzeniach i kontrolerach oraz

* Ustaw i zresetuj polecenia wydawane niewłaściwie.

36.1.5 Kontrola dostępu do systemu plików.

Systemy plików zapewniają kontrolę dostępu do danych. Systemy plików UNIX zapewniają kontrolki oparte na właścicielu użytkownika, właścicielu grupy i „innych” lub tych, którzy nie są użytkownikiem lub członkiem grupy będącej właścicielem danych. Systemy Microsoft R Windows umożliwiają określanie właścicieli danych i przyznawanie dostępu za pomocą indywidualnych nazw użytkowników lub kont grupowych. Listy kontroli dostępu (ACL) mogą również służyć do zapewniania wyjątków dostępu do normalnych uprawnień dostępu do plików danych. Po prawidłowym zastosowaniu te kontrole dostępu mogą skutecznie zapobiegać nieautoryzowanemu dostępowi do danych podczas normalnego użytkowania. Jednak system plików ufa kontrolom dostępu systemu operacyjnego komputera, aby poprawnie uwierzytelnić i autoryzować użytkownika. W przypadku obejścia kontroli dostępu do systemu operacyjnego kontrola dostępu do systemu plików traci swoją skuteczność. Aby uzyskać więcej informacji na temat systemu operacyjnego i kontroli dostępu do sieci lokalnej.

Kontrole systemu tworzenia kopii zapasowych i przywracania

Systemy używane do tworzenia kopii zapasowych i przywracania danych wymagają dodatkowej uwagi w zakresie bezpieczeństwa, ponieważ dane w nich zawarte są często krytyczne dla odtwarzania po awarii i ciągłości biznesowej. Istnieje kilka zagrożeń związanych z tworzeniem kopii zapasowych danych, które nie są narażone na ataki na inne magazyny danych. Podczas gdy większość systemów przechowuje dane tylko na dysku (DAS, NAS lub SAN), systemy tworzenia kopii zapasowych często zapisują dane na kasetach taśmowych lub innych nośnikach wymiennych przeznaczonych specjalnie do przechowywania poza siedzibą firmy. Inną opcją jest tworzenie kopii zapasowych danych w formie

elektronicznej w systemie zdalnym, w innym centrum danych organizacji lub u zewnętrznego dostawcy kopii zapasowych. Podobnie jak w przypadku każdej transmisji danych do odległych obiektów, dane muszą być chronione podczas tranzytu iw obiekcie docelowym. Niezależnie od użytego nośnika, wszystkie kopie zapasowe danych muszą być przechowywane w bezpiecznym, chronionym środowiskowo obiekcie dostatecznie oddalonym od miejsca pochodzenia, aby zminimalizować ryzyko utraty zarówno danych pierwotnych, jak i zapasowych w przypadku pojedynczego poważnego zdarzenia, takiego jak trzęsienie ziemi, powódź, lub erupcja wulkanu. Ponadto nośniki kopii zapasowych należy zabezpieczyć, ograniczając dostęp tylko do upoważnionego personelu. Nośniki używane do tworzenia kopii zapasowych muszą zostać ocenione, aby upewnić się, że spełniają lub przekraczają wymagania dotyczące długowieczności danych, określone przez zasady i standardy tworzenia kopii zapasowych organizacji. Należy również wziąć pod uwagę dodatkowe ryzyko związane z imitacją systemu. Jeśli atakujący jest w stanie wstawić system, który podszywa się pod system zapasowy, wszystkie dane, które mają zostać zarchiwizowane, mogą zamiast tego zostać zapisane bezpośrednio w systemie atakującego. I odwrotnie, jeśli atakujący jest w stanie wstawić system, który może podszywać się pod jeden lub więcej systemów przechowywania danych, wówczas atakujący może zażądać przywrócenia danych z istniejących kopii zapasowych, uzyskując nieautoryzowany dostęp do informacji. Aby złagodzić takie ryzyko, interakcje między systemami przechowywania danych a systemami tworzenia kopii zapasowych powinny być uwierzytelniane. W przypadku ręcznie sterowanych kopii zapasowych systemy mogą mieć utworzone konta kopii zapasowych, które wymagają interaktywnego logowania w celu uwierzytelnienia żądania kopii zapasowej. W przypadku automatycznych kopii zapasowych mogą być dostępne inne opcje, w tym użycie certyfikatów klienta i serwera do uwierzytelniania obu systemów biorących udział w kopii zapasowej. W ostatnich latach rozwój technologii przetwarzania w chmurze i przechowywania w chmurze umożliwił organizacjom wykorzystanie hybrydowych rozwiązań do tworzenia kopii zapasowych danych. Zamiast tworzyć kopie zapasowe danych w regularnych odstępach czasu, zmiany w systemach są replikowane do usługi opartej na chmurze w czasie zbliżonym do rzeczywistego, skutecznie działając jako zreplikowana kopia. Dodanie technologii deduplikacji, przesyłającej tylko te bloki danych ze zmianami, dodatkowo poprawia wydajność rozwiązania. Jednak, podobnie jak w przypadku wszystkich rozwiązań do zdalnego tworzenia kopii zapasowych, konieczna jest ciągła analiza due diligence z usługodawcą w celu zapewnienia, że istnieją odpowiednie zabezpieczenia w zakresie transmisji, przechowywania, dostępu i wyszukiwania danych. Jest to szczególnie ważne, biorąc pod uwagę charakter „na żądanie" rozwiązania opartego na chmurze lub rozwiązaniu hybrydowym do odzyskiwania danych lub systemu. Jakiekolwiek korzystanie z usług w chmurze powinno odbywać się dopiero po:

* Dokładnej ocenie praktyk bezpieczeństwa dostawcy usług w chmurze (CSP),

* Potwierdzeniu, że przechowywanie danych w rozwiązaniu jest zgodne ze wszystkimi wymogami prawnymi, regulacyjnymi i firmowymi oraz

* Stosowaniu szyfrowania danych, które utrzymuje wewnętrzne zarządzanie kluczami szyfrowania danych.

Przechowywanie danych poza siedzibą firmy, niezależnie od tego, czy są one zapisywane bezpośrednio na serwerze dostawcy pamięci masowej, czy na nośnikach wymiennych, takich jak taśma, zasługuje na własne względy bezpieczeństwa. Na przykład, w jaki sposób dostawca zabezpiecza fizyczny dostęp do swojej witryny? Jak sprawdzają swoich pracowników?

Większość takich zagrożeń można złagodzić, przeprowadzając analizę due diligence dostawcy przed zawarciem umowy oraz eliminując potencjalnych dostawców, którzy nie spełniają potrzeb organizacji w zakresie bezpieczeństwa. Inną strategią łagodzenia skutków jest szyfrowanie kopii zapasowych

danych przed wysłaniem ich poza siedzibę. Wiele aplikacji do tworzenia kopii zapasowych oferuje metody szyfrowania. Wykorzystanie szyfrowania plików i innych systemów przechowywania danych omówiono w dalszej części tego rozdziału. Podobne techniki można zastosować do kopii zapasowych danych, szyfrując je podczas zapisywania na nośniku kopii zapasowej

Ochrona interfejsów zarządzania

Interfejsy zarządzania stanowią jedno z największych zagrożeń dla bezpieczeństwa przechowywanych danych. Interfejsy te zapewniają dostęp administracyjny do magazynów danych, umożliwiając osobom o odpowiednim dostępie manipulowanie elementami danych, aktualizowanie zabezpieczeń kont i wykonywanie innych czynności porządkowych. Dlatego podczas wdrażania rozwiązania pamięci masowej należy zachować ostrożność, aby zapewnić, że istnieje dobrze zdefiniowana, dogłębna ochrona. Chociaż uwierzytelnianie dwuskładnikowe jest bezpieczniejsze, nie zawsze jest praktyczne. Jako absolutne minimum każdy użytkownik administracyjny powinien mieć zestaw poświadczeń i złożone wymagania dotyczące hasła, z regularną częstotliwością zmiany hasła. W sytuacjach, w których przechowywanie danych odbywa się za pośrednictwem źródła internetowego, uwierzytelnianie oparte na certyfikatach lub tokenach może zapewnić dodatkową warstwę zabezpieczeń uwierzytelniania. Ponadto osoby odpowiedzialne za administrowanie bezpieczeństwem nie powinny być tymi samymi osobami odpowiedzialnymi za zarządzanie środowiskiem pamięci masowej. Takie rozdzielenie obowiązków ogranicza możliwość obejścia kontroli bezpieczeństwa przez każdą osobę, bez pewnego rodzaju konspiracji między administratorami pamięci masowej i bezpieczeństwa. Innym ważnym elementem strategii obrony w głąb jest wykorzystanie dzienników kontroli. Rejestrowanie powinno być włączone w celu wykrywania naruszeń zasad i zalecanych procedur. Jednak dzienniki są bezwartościowe, chyba że są poddawane regularnej i losowej weryfikacji, z możliwością monitorowania w przypadku wykrycia anomalii. Nierealistyczne jest oczekiwanie, że ktoś codziennie przegląda obszerne pliki dziennika. Można jednak zastosować technologię agregacji logów i korelacji, aby zapewnić dodatkową warstwę pewności. Niezależnie od ostatecznej implementacji, korzystanie z dzienników kontrolnych i ograniczenia możliwości dostępu do tych dzienników i ich modyfikowania odgrywają ważną rolę w zapewnieniu, że nie doszło do uszkodzenia danych. Złagodzenie tych zagrożeń w interfejsie zarządzania wymaga starannego monitorowania i kontroli nad tym, kto może uzyskać dostęp do tych interfejsów i je zainstalować. Wraz z przejściem na interfejsy internetowe, dyskusja ta sprowadza się do ścisłej kontroli dostępu i uwierzytelniania użytkowników. W każdym razie konieczne jest, aby dostęp do interfejsu zarządzania mieli tylko zaufani użytkownicy, którzy muszą znać tę wiedzę. Po wejściu do środka ludzie mogą manipulować środowiskiem w razie potrzeby, aby wspierać swoje cele, czy to dla dalszych celów organizacyjnych, czy też do wykonywania złośliwych działań.

SŁABOŚCI I WYKORZYSTANIA KANAŁU FIBER

Kanały światłowodowe, choć bardzo ekonomiczne, stanowią wyjątkowe wyzwania dla środowiska pamięci masowej. Termin Fibre Channel odnosi się nie tylko do ścieżki komunikacyjnej opartej na światłowodzie, ale raczej do złożonego protokołu komunikacyjnego. Technologia ma szereg nieodłącznych słabości, z których niektóre są dość proste i łatwe do opanowania, ale inne wprowadzają pytania o wykonalność technologii w większych środowiskach pamięci masowej. Jedną z najpoważniejszych słabości zabezpieczeń w Fibre Channel jest to, że cała komunikacja odbywa się w postaci zwykłego tekstu. Na szczęście, gdy implementacja Fibre Channel odbywa się całkowicie w centrum danych lub innym zabezpieczonym obszarze, nie stanowi to większego problemu, ponieważ zdolność nieautoryzowanych osób do przechwytywania ruchu w sieci jest ograniczona, chyba że mają fizyczny dostęp do okablowania i mogą uniknąć wykrycia próbując przechwycić ruch lub zainstalować urządzenia przechwytujące. We wczesnej implementacji Fibre Channel natywne uwierzytelnianie i szyfrowanie nie były dostępne. Jednak nowsze przełączniki szkieletowe i urządzenia SAN zapewniają

wbudowane funkcje uwierzytelniania i szyfrowania, co znacznie zmniejsza ryzyko związane z transmisją danych w postaci zwykłego tekstu. Z perspektywy luk w zabezpieczeniach osoby atakujące mogą wykorzystać protokół internetowy (IP) do tworzenia exploitów przeciwko Fibre Channel, ponieważ oba protokoły wykorzystują schemat komunikacji oparty na ramkach. Niestety, w oparciu o omówioną powyżej kwestię zwykłego tekstu, osoba atakująca może podsłuchać ramki z połączenia Fibre Channel i uzyskać informacje potrzebne do przeprowadzenia ataku. Ta sekcja skupia się na trzech typach typowych ataków: człowiek w środku, przejmowanie sesji i uszkodzenie serwera nazw. Większość ataków na sieć pamięci masowej wymaga fizycznego dostępu do tego środowiska lub dostępu do odpowiedniego sprzętu podsłuchującego, co zwiększa trudność udanych, niewykrytych ataków.

Ataki Man-in-the-Middle

Ataki typu man-in-the-middle (MIMA) wykorzystują słabości komunikacji opartej na ramkach za pośrednictwem protokołu Fibre Channel. Podobnie jak ataki oparte na protokole IP, w atakach MIMA atakujący przechwytuje komunikację, kradnie lub zmienia dane i przekazuje tę ramkę do zamierzonego miejsca docelowego. Fibre Channel zawiera identyfikator sekwencji i liczbę sekwencji, które mają zapewnić spójną komunikację od nadawcy do odbiorcy. Podobnie jak IP, Sequence Count jest łatwo przewidywalną liczbą sekwencyjną, pozwalającą napastnikowi przewidzieć następny numer sekwencyjny i przesłać pakiet przed system wysyłający. Wprowadzony pakiet umożliwia atakującemu przechwycenie strumienia bez autoryzacji którejkolwiek ze stron. Złagodzenie tego problemu wymaga sprawdzenia integralności danych, aby zagwarantować odbiór prawidłowych informacji i odrzucenie fałszywych pakietów.

Przejęcie sesji

Przejmowanie sesji stwarza ten sam rodzaj problemu co MIMA i występuje w bardzo podobny sposób. Jednak ten typ ataku koncentruje się na braku uwierzytelniania w środowiskach Fibre-channel. Zamiast manipulować danymi w każdej ramce i przekazywać je dalej, haker wykorzystuje znajomość Sequence ID i Sequence Count do przechwytywania i kontrolowania sesji, sprawiając, że odbiorca wierzy, że atakujący jest naprawdę oryginalnym nadawcą. Nowo kontrolowana sesja może być następnie wykorzystana do wyodrębnienia dowolnych danych lub innych informacji, których zażąda atakujący. Łagodzenie tego problemu wymaga silnego uwierzytelniania, aby zagwarantować, że pierwotny nadawca jest nadal z tego samego systemu przez cały czas trwania połączenia.

Uszkodzenie serwera nazw

Ostatni typ ataku w tej sekcji obejmuje fałszowanie adresów, podobne do fałszowania adresów DNS w świecie IP. Każde połączenie Fibre-Channel rejestruje swoją nazwę w usłudze World Wide Name (WWN) za pomocą dwóch procesów, logowania do sieci Fabric (FLOGI) i logowania do portu (PLOGI). Zazwyczaj uszkodzenie serwera nazw występuje podczas procesu PLOGI przez umożliwienie niepoprawnemu hostowi zarejestrowania się w przełączniku Fibre Channel (który zawiera usługęWWN) przy użyciu sfałszowanego adresu. Przełącznik rejestruje hosta pod tym adresem tak, jakby był prawidłowy z powodu braku jakiegokolwiek uwierzytelnienia hosta. Gdy prawdziwy host próbuje się połączyć, przełącznik odmawia tego połączenia, ponieważ niepoprawny host jest już podłączony. Ten rodzaj ataku wymaga pewnego wyczucia czasu ze strony atakującego, ale może być łatwy do przeprowadzenia ze względu na omówione wcześniej słabości. Nowoczesne przełączniki szkieletowe zapewniają dodatkowe mechanizmy uwierzytelniania w celu ochrony przed tymi atakami poprzez weryfikację urządzenia z przełącznikiem w regularnych odstępach czasu.

Bezpieczeństwo kanału światłowodowego

Ta krótka analiza kanałów Fibre wykazała, że istnieje wiele słabości. Nie oznacza to jednak, że Fibre Channel należy odrzucić jako odpowiednią technologię. Wdrażając Fibre Channel w środowisku, należy zwrócić uwagę na te luki w zabezpieczeniach, biorąc pod uwagę lokalizację, odległość i dostępność wdrożenia dla osób, systemów i innych urządzeń w sieci. Fizyczne rozmieszczenie urządzeń i okablowania również musi być zoptymalizowane, aby ograniczyć ryzyko związane z używaniem kanałów światłowodowych. Sprzedawcy również odpowiadają na wezwanie, oferując technologię, która pomaga zabezpieczyć Fibre Channel dzięki wbudowanym funkcjom uwierzytelniania i szyfrowania.

SŁABE STRONY I WYKORZYSTYWANIA NFS.

Sieciowe systemy plików (NFS) zapewniają usługę pozwalającą użytkownikowi na komputerze klienckim na dostęp do zasobów sieciowych tak, jakby były one lokalne dla tego użytkownika. Ta usługa jest oparta na usłudze zdalnego wywoływania procedur (RPC) i chociaż jest bardzo przydatna w środowisku sieciowym, NFS przedstawia szereg problemów związanych z bezpieczeństwem, które należy rozwiązać przed wdrożeniem. NFS jest zwykle nastawiony na środowiska o dużej przepustowości, takie jak sieć LAN, lub sieci udostępniające niewrażliwe informacje. Ponieważ NFS nie zapewnia szyfrowania między hostami, korzystanie z tej technologii w innych sieciach, zwłaszcza tych z dostępem do Internetu, stwarza dodatkowe ryzyko. W tej sekcji opisano trzy najczęstsze słabości i luki w zabezpieczeniach systemu plików NFS: uprawnienia użytkowników i plików, zaufane hosty i przepełnienia bufora.

Uprawnienia użytkownika i pliku

Oprócz braku szyfrowania, NFS umożliwia dostęp użytkownika na podstawie konkretnego hosta podłączonego do udziału NFS. Oznacza to, że każdy użytkownik podłączony do tego hosta może uzyskać dostęp do zasobów sieciowych. Ograniczenie użytkownikom dostępu tylko do odczytu eliminuje możliwość używania NFS jako technologii współpracy, ponieważ użytkownicy nie mogą już tworzyć ani aktualizować informacji o udziałach. Podczas montowania udziałów z dostępem do odczytu i zapisu w systemie NFS każdy użytkownik podłączony do hosta może uzyskać dostęp do plików innego użytkownika, ponieważ jedyną ochroną, jaką ma plik, są jego uprawnienia. Administratorzy próbują ograniczyć to ryzyko, zmuszając wszystkich użytkowników do uzyskania dostępu do udziału w ramach grupy lub wspólnego zestawu poświadczeń tylko do odczytu, ale takie podejście eliminuje niektóre korzyści, jakie zapewnia udział sieciowy. Udział tylko do odczytu wymaga od administratorów aktualizacji lub edytowania plików, co zapewnia podejście przypominające bibliotekę, a nie wspólne środowisko zarządzania plikami.

Zaufane hosty

Problemy z NFS dotyczą w szczególności uwierzytelniania hostów w środowisku NFS. Ponieważ NFS kontroluje żądania montowania na podstawie połączenia hosta, a nie konkretnego użytkownika, nieuczciwy host może zażądać montowania NFS i wprowadzić zmiany w zasobach. Osoba atakująca może również złamać serwer DNS używany przez system eksportujący system plików NFS, aby skierować ten system do nieautoryzowanego komputera. Ponieważ przed zamontowaniem udziałów NFS nie są udostępniane żadne poświadczenia logowania, jeśli hosty nie są zaufane, nie ma żadnych dodatkowych testów sprawdzających integralność nowego hosta.

Przepełnienie bufora

W wielu implementacjach NFS sprawdzanie wprowadzania danych nie odbywa się przed przetworzeniem żądania. Ta usterka stwarza okazję do ataku z przepełnieniem bufora. Gdy do serwera

NFS przychodzi żądanie usunięcia katalogu od użytkownika z uprawnieniami do odczytu i zapisu, serwer nie sprawdza długości nazwy ścieżki, a użytkownik może dołączyć dodatkowe instrukcje wykraczające poza to, co powinien otrzymać serwer. Te instrukcje, przypuszczalnie złośliwe, mogą być następnie wykonywane przez serwer jako konto administracyjne, takie jak root lub administrator. W rezultacie może dojść do niezamierzonej lub nieautoryzowanej manipulacji danymi. Najnowsze implementacje NFS zawierają uwierzytelnianie Kerberos, aby pomóc w weryfikacji użytkowników i ich możliwości. Ponadto ta sama walidacja może być użyta do walidacji hostów przed połączeniem się z serwerem NFS. Jednak te ulepszenia to tylko częściowe rozwiązania. Hakerzy kryminalni nadal opracowują i stosują nowe przepełnienia bufora, więc nierozsądne byłoby zakładanie, że NFS lub jakakolwiek inna technologia sieciowa może być całkowicie zabezpieczona. Bardziej szczegółowe omówienie bezpiecznych technik programowania i zapewniania jakości oprogramowania w celu uniknięcia przepełnienia bufora oraz identyfikowania i zapobiegania innym lukom w oprogramowaniu można znaleźć w rozdziałach 38 i 39 tego podręcznika.

WYKORZYSTANIA CIFS

Common Internet File System (CIFS), protokół bloku komunikatów serwera z obsługą Internetu (SMB), opiera się na tym protokole, włączając szyfrowanie i bezpieczne uwierzytelnianie do istniejących możliwości udostępniania zasobów SMB. Niestety, z punktu widzenia bezpieczeństwa CIFS łączy niektóre nowe elementy z niektórymi starymi, czego wynikiem jest szereg problemów związanych z bezpieczeństwem.

Uwierzytelnianie

Implementacje CIFS zapewniają prosty schemat uwierzytelniania oparty na hasłach lub schemat wyzwania-odpowiedzi. Oba te podejścia występują w postaci zwykłego tekstu, co pozwala każdemu, kto ma dostęp przewodowy, na przechwycenie i przechwycenie poświadczeń uwierzytelniania w udziale sieciowym. Nawet przy podejściu wyzwanie-odpowiedź napastnicy mogą sfałszować transakcję i uzyskać dostęp do udziału. Ostatnie implementacje CIFS opierają się na protokole Kerberos do uwierzytelniania i podobnie jak NFS, zapewniając dodatkowe zabezpieczenia, wprowadzają luki oparte na protokole Kerberos, które wykraczają poza zakres tej sekcji. Niektóre implementacje CIFS zapewniają również model bezpieczeństwa „na poziomie udziału", a nie model bezpieczeństwa „na poziomie użytkownika". Zasadniczo, zamiast każdego użytkownika utrzymującego indywidualne poświadczenia, udział ma tylko jeden zestaw poświadczeń, który udostępniają wszyscy użytkownicy. Słabości nieodłącznie związane z modelem na poziomie udziałów są podobne do tych stwierdzonych przy użyciu kont grupowych lub współdzielonych w dowolnym innym systemie. Oprócz problemów z uwierzytelnianiem, CIFS jest również podatny na ataki słownikowe i brute-force na dane uwierzytelniające użytkownika. Zazwyczaj obejmują one atak z wybranym tekstem jawnym, wspomagany przez przechwytywanie par wyzwanie-odpowiedź podczas procesu uwierzytelniania. Jednak zarówno ataki słownikowe w trybie online, jak i offline są dostępne dla atakującego w zależności od ilości czasu dostępnego do oglądania prób połączenia.

Nieuczciwi lub podrabiani gospodarze

Ważne jest, aby zidentyfikować różnice między powierzchnią ataku CIFS i NFS. Problemy typu „man-in-the-middle" i „zaufany host" dotyczą zarówno CIFS, jak i innych problemów. Niewłaściwie skonfigurowani klienci CIFS mogą zostać oszukani, myśląc, że powinni podać hasło zamiast wchodzić w interakcję ze scenariuszem wyzwania-odpowiedź, wspierając w ten sposób ataki typu man-in-the-middle. Ponadto, jeśli środowisko CIFS, które nie umożliwia uwierzytelniania sesji lub wiadomości, usuwa mechanizmy zabezpieczeń zaprojektowane specjalnie do ochrony przed tego typu atakami. CIFS ma wiele takich samych problemów z bezpieczeństwem, co NFS. Jednak większości problemów można

uniknąć, włączając funkcje bezpieczeństwa zawarte w protokole. Ataki typu man-in-themiddle i przejmowanie sesji, oprócz ataków polegających na powtarzaniu i fałszowaniu, można uniknąć dzięki uwierzytelnianiu wiadomości i sesji. Nie oznacza to, że CIFS może być całkowicie zabezpieczony, ale należy zachować ostrożność na etapie konfiguracji implementacji, aby wykorzystać wszystkie dostępne mechanizmy bezpieczeństwa.

SZYFROWANIE

Wiele osób i organizacji koncentruje się na szyfrowaniu danych w ruchu, sieciach tranzytowych i Internecie. Sposób użycia szyfrowania danych w stanie spoczynku lub podczas przechowywania jest równie ważne. Jak wspomniano wcześniej, przechowywane dane są częściej zagrożone przez naruszenia bezpieczeństwa niż dane w trakcie przesyłania. Przy użyciu wystarczająco silnego algorytmu i odpowiednio dobranego klucza dane przechowywane w postaci zaszyfrowanej mogą stać się bezużyteczne dla osób, które nie mają możliwości odszyfrowania danych. Nawet jeśli atak zakończy się sukcesem, aby uzyskać pełną kontrolę nad kopią danych w przypadku prób deszyfrowania metodą brute force, odpowiedni algorytm i klucz mogą uniemożliwić odszyfrowanie danych przez wystarczająco długi okres – wystarczająco długi, aby jakiekolwiek informacje umożliwiające identyfikację osób (PII) lub inne wrażliwe, poufne lub zastrzeżone informacje nie miałyby żadnej wartości, z wyjątkiem historyków. Gdy system zostanie zgubiony lub skradziony, osoba atakująca ma zasadniczo nieograniczoną ilość czasu na uzyskanie dostępu do danych. Jeśli dane nie są zaszyfrowane, można je po prostu odczytać po ustaleniu identyfikatora użytkownika i hasła. Jeśli złamanie kontroli dostępu do systemu operacyjnego nie powiedzie się, niezaszyfrowany dysk twardy można po prostu odczytać na innym komputerze za pomocą systemu plików lub, jeśli nie jest to możliwe, za pomocą narzędzi śledczych. W przypadku zaszyfrowanych systemów plików lub szyfrowania woluminów tylko część danych jest przechowywana w postaci zaszyfrowanej. Dane, które nie znajdują się w jednej z tych zaszyfrowanych lokalizacji, są podatne na ataki - w tym przestrzenie wymiany i tymczasowe lokalizacje plików używane przez system operacyjny.

Odzyskiwalność

Kluczowe zasady zapewniania informacji (IA) obejmują ochronę dostępności i użyteczności danych. Ze swej natury szyfrowanie może usunąć te zabezpieczenia w zamian za ochronę autentyczności, poufności i integralności danych, jednocześnie zmniejszając ryzyko utraty danych. Podczas korzystania z szyfrowania danych należy wziąć pod uwagę możliwą potrzebę odzyskania danych w przypadku, gdy nie można zlokalizować użytkownika lub klucza podstawowego. Jest na to kilka sposobów. Depozyt klucza jest jedną z metod ułatwiających odzyskiwanie zaszyfrowanych danych. Przechowując klucz u zaufanej strony, utracony klucz można usunąć z depozytu i wykorzystać do odszyfrowania danych. W przypadku szyfrowania kluczem publicznym można użyć dodatkowych kluczy odszyfrowywania (ADK) z niektórymi narzędziami szyfrującymi. Korporacyjne zestawy ADK to klucze, których można używać podczas procesu szyfrowania do automatycznego szyfrowania danych za pomocą klucza, który jest ściśle kontrolowany i używany tylko przez wyznaczone osoby do odzyskiwania zaszyfrowanych danych.

Szyfrowanie plików

Stosowanie szyfrowania na zasadzie plik po pliku jest dobrą metodą zabezpieczania danych. Dzięki szyfrowaniu plików użytkownik może wybrać i wybrać pliki do zaszyfrowania. Pliki zawierające dane wrażliwe mogą być szyfrowane, natomiast pliki niewrażliwe są przechowywane bez szyfrowania. Ma to najmniejszy wpływ na system, ale największą odpowiedzialność spoczywa na użytkowniku, który musi określić, które pliki powinny być zaszyfrowane. Pliki systemu operacyjnego nie mogą być zaszyfrowane, więc pliki konfiguracyjne, które mogą zawierać informacje o systemach organizacji, są traktowane jako ryzykowne – podobnie jak pliki kodu aplikacji. Te pliki kodu mogą dotyczyć

zastrzeżonej aplikacji organizacji, która zapewnia znaczną przewagę konkurencyjną. Jednak takie pliki rzadko są szyfrowane, ponieważ może to stanowić przeszkodę dla użytkownika, który musi pamiętać o odszyfrowaniu każdego pliku, gdy jest to wymagane.

Szyfrowanie woluminów i systemy szyfrowania plików

Zarówno szyfrowanie woluminów, jak i systemy szyfrowania plików zapewniają ochronę danych i mogą być łatwiejsze dla użytkowników niż szyfrowanie na plik. Łatwość użycia wynika z jednej operacji wymaganej do uzyskania dostępu do wielu plików. W zależności od konfiguracji lokalizacja może pozostać odszyfrowana i dostępna przez kilka minut lub kilka godzin. Krytyczna różnica między szyfrowaniem plików a szyfrowaniem woluminów polega na tym, że odszyfrowywanie odbywa się na poziomie sterownika, gdy dane są przenoszone z dysku do pamięci RAM. Cały wolumin nie jest odszyfrowywany. Jednak wejścia/wyjścia (we/wy) do iz zamontowanego woluminu mogą być znacznie wolniejsze niż z niezaszyfrowanego dysku. Ponadto dynamiczne odszyfrowywanie zapewnia, że w przypadku przerwania zamykania systemu nie ma obszernej, jawnej wersji oryginalnych materiałów przechowywanych na dysku twardym lub w pamięci wirtualnej do analizy kryptograficznej. W przypadku częściowego szyfrowania przy użyciu szyfrowania plików lub zaszyfrowanych woluminów chroniona jest tylko część danych przechowywanych na dysku i specjalnie zapisanych na zaszyfrowanej partycji. Zazwyczaj pliki systemu operacyjnego i aplikacji nie są zaszyfrowane, więc skradziony lub w inny sposób naruszony dysk jest podatny na ataki atakujących, którzy uzyskaliby dostęp do dowolnego pliku, który nie został zapisany w zaszyfrowanym woluminie lub systemie plików. Jeśli użytkownik zapomni zaszyfrować plik lub folder zawierający poufne dane, wówczas te niezabezpieczone dane są dostępne dla każdego, kto może uzyskać dostęp do systemu operacyjnego lub odczytać dysk twardy za pomocą narzędzi śledczych lub innych narzędzi dyskowych.

Pełne szyfrowanie dysku

Autor Ryan Groom wymienia przekonujące powody używania pełnego szyfrowania dysku na laptopach. Można je powtórzyć dla dowolnego systemu. Głównym powodem korzystania z pełnego szyfrowania dysku jest to, że:

* Chroni dane w przypadku zgubienia lub kradzieży dysku,

* jest bezpieczniejszy i skuteczniejszy niż szyfrowanie woluminów lub systemy szyfrowania plików,

* Może być przejrzysty dla użytkowników i

* Pomaga zachować zgodność z kwestiami prawnymi i regulacyjnymi.

Pełne szyfrowanie dysku zabezpiecza system plików i pliki systemu operacyjnego, ale pozostawia niewielką część rozruchową dysku niezaszyfrowaną. Region niezaszyfrowany umożliwia ładowanie oprogramowania szyfrującego, żądanie hasła, hasła lub tokena potrzebnego do zainicjowania dynamicznego odszyfrowywania zawartości dysku na żądanie oraz kontynuowania ładowania systemu operacyjnego. W zależności od wybranego rozwiązania użytkownicy mogą zauważyć niewielką różnicę w funkcjonalności lub wydajności między systemem wykorzystującym pełne szyfrowanie dysku a systemem, który tego nie robi. Podstawowa widoczność dla użytkowników polega na tym, że podczas rozruchu systemu użytkownik musi zidentyfikować i uwierzytelnić się, aby umożliwić odszyfrowanie i kontynuować rozruch systemu. Wydajność systemu jest prawie niezauważalnie zmniejszona, z niewielkimi opóźnieniami podczas uruchamiania systemu, podczas gdy znaczna ilość programów systemu operacyjnego i danych z dysku jest odszyfrowywana, a także ponownie po zamknięciu, gdy niezaszyfrowane dane są czyszczone, aby uniemożliwić czytelność bez autoryzacji. Chociaż operacje we/wy mogą być wolniejsze niż w systemach niezaszyfrowanych, większość operacji dostępu do plików

nie wymaga dużej ilości operacji we/wy, więc ogólnie rzecz biorąc, te minimalne skutki dla użytkowników są znacznie niwelowane przez ochronę zapewnianą przez pełne szyfrowanie dysku. Podobnie jak w przypadku szyfrowania woluminów, pełne szyfrowanie dysku obejmuje dynamiczne odszyfrowywanie tekstu zaszyfrowanego, gdy przepływa on z dysku do buforów pamięci. Przy nowoczesnych szybkościach przesyłania danych i możliwościach procesora wszelkie opóźnienia w wydajności spowodowane odszyfrowywaniem w locie po załadowaniu systemu operacyjnego są w praktyce znikome.

Dzięki pełnemu szyfrowaniu dysku cała zawartość dysku jest chroniona. Nawet przy pełnym fizycznym dostępie do dysku (np. instalując go na innym komputerze pod kontrolą atakującego) lub z kopią bit po bicie zaszyfrowanego dysku, atakujący musi złamać szyfrowanie, aby uzyskać jakiekolwiek informacje – prawie niemożliwe zadanie przy aktualnie używanych rozmiarach kluczy, z wyjątkiem być może rządowych laboratoriów kryptoanalizy używających masowo równoległych architektur do łamania metodą brute-force. Dzięki silnemu szyfrowaniu kierownictwo może być w stanie zaspokoić obawy klientów, jeśli organizacja musi ujawnić utratę sprzęt i musi zapewniać, że nawet jeśli dysk został utracony, dane klienta i organizacji nie będą dostępne.

Luka dotycząca szyfrowania woluminów, systemu plików i pełnego dysku.

Tak silna jak ochrona zapewniana przez wolumin, system plików i pełne szyfrowanie dysku, jest jedna istotna słabość. Gdy użytkownik jest upoważniony do dostępu do danych, a system operacyjny dynamicznie odszyfrowuje dane zgodnie z wymaganiami, system jest podatny na ataki ze strony każdego intruza, który ma fizyczny dostęp do odblokowanej, niechronionej sesji. Na przykład, jeśli system zawiera wrażliwe dane i jest podłączony do sieci, każdy atak przez sieć może potencjalnie narazić dane, gdy sesja autoryzowanego użytkownika umożliwia dostęp do odszyfrowanych danych. Tę lukę należy podkreślić w przypadku użytkowników, którzy mogą niewłaściwie zrozumieć konsekwencje szyfrowania, zwłaszcza tych, którzy nalegają na przechowywanie poufnych danych na swoich laptopach. Podczas gdy pełne szyfrowanie dysku chroni dane, gdy system nie jest uruchamiany, gdy użytkownik odszyfruje dysk podczas uruchamiania, dane są dostępne nie tylko dla niego, ale dla każdego, kto uzyska dostęp do systemu. Systemy muszą stosować szczegółowe strategie obrony z osobistymi zaporami sieciowymi, aby zapobiegać nieautoryzowanemu dostępowi do systemu przez sieć; użytkownicy muszą fizycznie posiadać system, zwłaszcza po wprowadzeniu klucza deszyfrującego. Jeśli użytkownik z systemem operacyjnym Windows na laptopie zablokuje ekran, a następnie odchodzi, dane są chronione tylko siłą hasła systemowego. Szczególnie wrażliwe dane powinny być szyfrowane na poziomie plików. Alternatywnie można użyć szyfrowania woluminu i systemu plików z rozsądnymi limitami czasu. Obie te opcje zapewniają zwiększoną ochronę danych podczas uruchamiania systemu. W połączeniu z pełnym szyfrowaniem dysku znacznie zmniejsza się ryzyko dla danych. Niektóre aplikacje oferują opcje szyfrowania danych (np. MS-OUTLOOK zawiera opcje szyfrowania plików PST zawierających wszystkie dane użytkownika). A co może być gorsze dla atakującego, który łamie pełne szyfrowanie dysku tylko po to, by odkryć, że informacje są superszyfrowane na jednym lub kilku poziomach, jeśli szyfrowanie plików, szyfrowanie woluminów i pełne szyfrowanie dysku są w użyciu? Ważnym punktem w dyskusji na temat szyfrowania wielopoziomowego jest to, że wymaga od organizacji silnego zaangażowania we wspieranie bezpieczeństwa na tym poziomie. Pełne szyfrowanie dysku można włączyć na poziomie globalnym za pomocą zasad grupy lub innych rozwiązań opartych na technologii. Jednak, jak wspomniano powyżej, użytkownik musi selektywnie wybrać szyfrowanie danych wrażliwych, zrzucając na nich odpowiedzialność i odpowiedzialność. Jednak przy podejściu do szyfrowania wielowarstwowego nadal istnieje warstwa ochrony przed zapomnieniem lub celowym unikaniem zaszyfrowania poufnych danych przez użytkownika. W ciągu ostatnich kilku lat powstało wiele przepisów dotyczących prywatności danych, w tym różne przepisy obowiązujące w większości

stanów USA i Unii Europejskiej. Wiele z tych przepisów wymaga powiadomienia użytkowników, których to dotyczy, w przypadku utraty danych. Jednak wiele z tych przepisów obejmuje „bezpieczną przystań" od powiadomienia, jeśli dane zostały zaszyfrowane na zgubionym lub skradzionym urządzeniu lub nośniku. (Autorzy zdecydowanie zalecają skonsultowanie się z radcą prawnym w celu właściwej interpretacji przepisów obowiązujących w Twojej jurysdykcji i/lub jurysdykcji wszelkich podmiotów danych, których potencjalnie dotyczy naruszenie lub utrata danych).

Szyfrowanie bazy danych

Dla wielu organizacji bazy danych, które są główną lokalizacją przechowywania danych, są również doskonałym celem atakujących. Dzięki zastosowaniu szyfrowania bazy danych można znacznie wydłużyć czas potrzebny napastnikowi na uzyskanie dostępu. Bazy danych można chronić, umieszczając je w systemie, do którego można uzyskać dostęp tylko za pośrednictwem bezpiecznego połączenia i który wykorzystuje szyfrowanie woluminów lub pełnego dysku. Ponadto istnieją funkcje szyfrowania bazy danych lub narzędzia zewnętrzne zaprojektowane w celu ochrony danych przechowywanych w tych sklepach, nawet bez szyfrowania dysku. Narzędzia te wykorzystują szyfrowanie w polu (pojedynczy element danych), wierszu (zbiór pól, które są wyrównane w wierszu w widoku tabelarycznym) oraz pełne szyfrowanie bazy danych. Jedną z zalet szyfrowania specyficznego dla bazy danych jest to, że może wspierać ścisłą zgodność z wymogami prawnymi dotyczącymi ochrony danych. Na przykład dane umożliwiające identyfikację, takie jak nazwiska, numery PESEL, informacje medyczne itd., mogą być chronione na najwyższym dostępnym poziomie bezpieczeństwa na wypadek, gdyby nieupoważniony personel lub intruzi uzyskali dostęp do bazy danych. James C. Foster w artykule dla SearchSecurity.com stwierdził, że organizacje „często przeskakują na szyfrowanie baz danych jako szybką naprawę zgodności bez uwzględnienia kilku kluczowych czynników. Największym z tych czynników jest szybkość lub wydajność aplikacji, ponieważ źle zaimplementowane szyfrowanie bazy danych może mieć wpływ na aplikacje produkcyjne". Foster zaleca cztery „proste wskazówki, które pomogą zabezpieczyć bazę danych bez utrudniania działalności, którą próbujesz chronić", które są rozwinięte poniżej:

* Nie szyfruj kluczy obcych ani superkluczy. Klucze te są używane do indeksowania, a ich szyfrowanie może negatywnie wpłynąć na użyteczność bazy danych. Ponieważ klucze te nie są zaszyfrowane, klucze nigdy nie powinny zawierać informacji, które powinny być chronione — na przykład numeru ubezpieczenia społecznego klienta lub numeru karty kredytowej jako klucza do łączenia tabel.

* Podobnie jak w przypadku każdego zastosowania szyfrowania, algorytmy symetryczne są szybsze niż klucze asymetryczne. Jeśli jednak wszystkie dane są zaszyfrowane jednym kluczem, klucz ten musi być dobrze chroniony, w przeciwnym razie osoba atakująca, która go znajdzie, może, całkiem dosłownie, mieć klucz do królestwa głównego magazynu danych organizacji.

* „Pełne szyfrowanie bazy danych jest rzadko zalecane lub jest wykonalną opcją. Najlepsze praktyki w zakresie bezpieczeństwa nauczą Cię szyfrowania wszystkiego za pomocą wielu kluczy i różnych algorytmów". Jednak personel techniczny powinien ocenić wpływ na wydajność.

* „Szyfruj tylko poufne dane [kolumny]. To zazwyczaj wszystko, czego wymagają lub zalecają przepisy, a przecież to wymaga ochrony".

Ulepszanie opcji dostarczanych przez dostawcę

Dostawcy baz danych, tacy jak Oracle Corporation i Microsoft, oferują opcje szyfrowania, które są specjalnie zaprojektowane w celu ochrony informacji w ich bazach danych. Opcje te z czasem uległy poprawie i stają się bardziej solidne i dojrzałe. Microsoft SQL Server 2005 oferuje ulepszenia

szyfrowania kolumn. Wprowadzono również „zintegrowaną i hierarchiczną infrastrukturę do zarządzania kluczami szyfrowania". Dokumentacja produktu kontynuuje: „Wbudowane funkcje szyfrowania i interfejsy programowania aplikacji (API) ułatwiają organizacji tworzenie ram bezpieczeństwa szyfrowania". Oracle Database 10g Release 2 ulepsza istniejące opcje szyfrowania w bazach danych Oracle, wprowadzając transparentne szyfrowanie danych (TDE). Korzystając z TDE, administrator bazy danych może określić, że kolumna musi być zaszyfrowana, a baza danych automatycznie szyfruje dane podczas operacji wstawiania i odszyfrowuje dane podczas wybierania. Można to osiągnąć „bez pisania ani jednej linii kodu". Arup Nanda przedstawia dobry przegląd tej funkcji w wydaniu magazynu Oracle z września/października 2005 roku.

Rozważania dotyczące implementacji

Podobnie jak w przypadku każdej implementacji szyfrowania, należy dokładnie rozważyć określenie metody i procesu wdrażania rozwiązania, a także szyfrowanych danych. Należy unikać szyfrowania pola klucza. Jeśli wrażliwe dane znajdują się w polu klucza, może być wymagana znaczna praca w celu utworzenia nowych pól klucza i odtworzenia powiązań tabeli lub organizacja może zdecydować się zaakceptować pogorszenie wydajności, które może wystąpić podczas szyfrowania pola klucza. Oznacza to, że przy założeniu, że zaszyfrowanie pola klucza nie spowoduje, że baza danych stanie się bezużyteczna.

Koszty związane z wdrożeniem szyfrowanego rozwiązania bazodanowego należy również porównać z ryzykiem biznesowym. W przypadku firm, które mają niewiele danych wymagających szyfrowania, szyfrowanie bazy danych może być nieodpowiednie. Wymagania prawne i regulacyjne należy również wziąć pod uwagę, ponieważ szyfrowanie bazy danych może być obowiązkowe w celu ochrony danych i uniknięcia odpowiedzialności karnej lub cywilnej. Towarzysząca temu utrata zaufania opinii publicznej i klientów w przypadku naruszenia bezpieczeństwa danych jest również potężną zachętą.

Szyfrowanie smartfona

Użytkownicy mogą przechowywać poufne informacje na telefonach komórkowych i tabletach; Typowe wpisy obejmują wpisy kontaktowe z numerami telefonów, a czasami z dodatkowymi danymi wrażliwymi, takimi jak hasła, informacje umożliwiające identyfikację osoby (np. numery identyfikacyjne wydane przez rząd) i rejestry połączeń. Takie urządzenia mogą być również używane tak, jakby były dyskami flash, z potencjalnie gigabajtami poufnych danych pobranych z innych źródeł i noszonymi w kieszeni, teczce lub torebce – a zatem łatwo ukraść lub zgubić. Innym czynnikiem, który może mieć znaczenie dla niektórych użytkowników, jest to, że zgodnie z prawem amerykańskim w momencie pisania tego dokumentu (w czerwcu 2013 r.) podejrzany, który jest przesłuchiwany, przesłuchiwany lub aresztowany, nie może normalnie zostać zmuszony do ujawnienia kodu deszyfrującego. Telefony korzystające z systemu Android 2.3.4 lub nowszego są zwykle wyposażone w zintegrowane szyfrowanie całkowite; proces trwa zwykle około godziny, najlepiej rozpoczyna się od w pełni naładowanego akumulatora i podłączenia do źródła zasilania i nie wolno go przerywać. Przerwanie tego procesu szyfrowania może uszkodzić lub usunąć dane przechowywane w telefonie i wymaga przywrócenia ustawień fabrycznych, które usuwa wszystkie bieżące dane i ustawienia osobiste z urządzenia. Apple iOS i Microsoft Windows Phone 7 zawierają również funkcje szyfrowania ze zróżnicowanym zasięgiem. Oprogramowanie innych firm jest dostępne dla wszystkich systemów operacyjnych omówionych powyżej. W marcu 2013 roku naukowcy z Uniwersytetu Friedrich-Alexander odkryli, jak uzyskać dostęp do danych zaszyfrowanych w wersji systemu operacyjnego Android:

Zespół zamroził telefony na godzinę, aby obejść system szyfrowania, który chroni dane w telefonie poprzez ich zaszyfrowanie… Atak pozwolił naukowcom uzyskać dostęp do list kontaktów, historii

przeglądania i zdjęć… [Wprowadzili] Telefony z Androidem w zamrażarce przez godzinę, aż urządzenie ostygnie poniżej -10 C.… [Szybkie] podłączenie i odłączenie baterii zamrożonego telefonu zmusiło słuchawkę do przejścia w tryb wrażliwy. Ta luka pozwala im uruchomić go z jakimś niestandardowym oprogramowaniem, a nie z pokładowym systemem operacyjnym Android. Naukowcy nazwali swój niestandardowy kod Frost - Forensic Recovery of Scrambled Telephones.

USUWANIE DANYCH

Ostatnią kwestią związaną z zabezpieczeniem przechowywanych danych jest usunięcie nośnika zawierającego dane. Wskazówki dotyczące odkażania nośników elektronicznych można znaleźć w normie 5220.22-M Departamentu Obrony Stanów Zjednoczonych. Zasadniczo nośniki należy odkazić, aby nie można było odzyskać zapisanych na nich danych. Jedna metoda osiągnięcia tego celu może obejmować następujące kroki:

1. Usuń dane

2. Zapisuj do mediów losowe lub nic nieznaczące dane

3. Usuń dane

4. Powtarzaj, aż do osiągnięcia pożądanego poziomu odkażania

W przypadku informacji przechowywanych na papierze papier należy co najmniej rozdrobnić przed wyrzuceniem. Korzystanie z niszczarki poprzecznej jest konieczne, ponieważ zwiększa to trudność ponownego składania dokumentów. W jednym głośnym incydencie, konfetti zbadane po tym, jak zostało rzucone podczas parady z okazji Święta Dziękczynienia w Nowym Jorku w 2012 roku, okazało się łatwe do odczytania poziome strzępy poufnych akt z Departamentu Policji hrabstwa Nassau. „Były całe wyroki, numery rejestracyjne i raporty policyjne". Istnieją dodatkowe kroki, które można podjąć w razie potrzeby, a dostępne są urządzenia do ich wykonania, w tym spalanie poszatkowanego papieru i mieszanie go z wodą, aby przyspieszyć jego degradację. W ciągu ostatnich kilku lat sprzedawcy specjalizujący się w niszczeniu papieru na miejscu stali się powszechni. Sprzedawcy ci przywożą ciężarówki do siedziby klienta i zbierają papier, który jest następnie rozdrabniany na miejscu, zanim zostanie przewieziony do zakładu, który przetwarza, spala lub w inny sposób usuwa odpady w bezpieczny sposób.

UWAGI KOŃCOWE

Bezpieczeństwo przechowywanych danych ma kluczowe znaczenie. Więcej naruszeń danych występuje w przypadku danych w niezabezpieczonych lokalizacjach przechowywania niż jest zagrożone podczas transportu. Przy odpowiednim bezpieczeństwie przechowywania danych istnieje mniejsze ryzyko dla danych ze strony wszelkiego rodzaju zagrożeń, wewnętrznych i zewnętrznych. Korzystanie z bezpiecznych kanałów do zapisywania danych na dysku i ochrony samych dysków ma coraz większe znaczenie, ponieważ atakujący zwykle mają jeden z dwóch celów - spowodowanie, że systemy lub dane staną się niedostępne, lub naruszy poufność i integralność danych. Łącząc bezpieczne kanały komunikacji, szyfrowanie danych w spoczynku i fizyczną ochronę urządzeń do przechowywania danych, można lepiej zapewnić bezpieczeństwo informacji.