

# Audyty systemów bezpieczeństwa informacji

Czułość popłaca



**Masa informacji wpływa do przedsiębiorstwa, jednak kluczowa jest kontrola nad danymi, które z niego wypływają. To złożone zadanie. Dodatkowo trzeba się liczyć z tym, że przechowywane wewnątrz organizacji informacje mogą być narażone na ataki z zewnątrz. Sprawny i cyklicznie aktualizowany system zarządzania bezpieczeństwem informacji to skuteczna bariera obronna przed niepożądanym wpływem danych.**

## Co mówi prawo i ISO

Kwestie bezpieczeństwa informacji i tajemnicy przedsiębiorstwa są regulowane przez prawo. O tajemnicy przedsiębiorstwa wspomina art. 11 ust. 4. ustawy o zwalczaniu nieuczciwej konkurencji: „Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności”.

Jak widać, prawo pozostawia dużą swobodę i swerrenność w kształtowaniu działań, które mają zapewnić poufność informacji. Najczęściej działania te obejmują różnego rodzaju formy identyfikowania dokumentów, grupowanie ich w kategorie oraz znakowanie znanym z filmów określeniem „ściśle tajne”. Dalej jest to definiowanie zasad i procedur, które będą obejmować konkretną wiedzę będącą w posiadaniu przedsiębiorstwa.

Złożoność takich procesów może przybrać znaczne rozmiary i wówczas doświadczenie firmy, czyli tzw. nauka na błędach, może być wspomagane przez najlepsze praktyki wdrożonych norm ISO 27001, jak również pomoc narzędzi informatycznych.

Norma ISO/IEC 27001 została opublikowana 14 października 2005 r. na podstawie brytyjskiego standardu BS 7799-2, a w roku 2007 rozszerzona przez normę ISO/IEC 27002 (nazywaną również ISO/IEC 17799). Normy te określają 11 obszarów mających wpływ na bezpieczeństwo informacji. Zbudowanie systemu zarządzania bezpieczeństwem informacji opartego na normach ISO wymaga szerokiego spojrzenia zarówno na obszary osobowe, fizyczne i środowiskowe, jak również bezpieczeństwo dokumentów, ich obrót czy infrastrukturę i systemy teleinformatyczne.

### Po pierwsze świadomość zagrożenia

Systemy zarządzające informacjami w przedsiębiorstwach są narażone na różnorakie zagrożenia wynikające zarówno z pośrednich ataków poprzez nieświadomych niczego pracowników, jak i ataków bezpośrednio na infrastrukturę teleinformatyczną. Pierwszym i najważniejszym etapem analizy ryzyka i budowania zabezpieczeń jest uświadomienie sobie zagrożenia.

Należy podkreślić, że chodzi tutaj zarówno o świadomość na poziomie całego przedsiębiorstwa, jak i pojedynczego pracownika. Nawet jeśli uważamy, że przechowywane dane nie są na tyle cenne, by warto było inwestować w systemy zabezpieczeń, trzeba mieć świadomość, że kradzież danych to tylko jedno z możliwych niebezpieczeństw.

Niezabezpieczona sieć może stać się częścią botnetu, czyli grupy komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem. A po ataku hakera policja zapuka do naszych drzwi. W przypadku przedsiębiorstwa konsekwencje takiej nonszalancji mogą być dotkliwe, dlatego aby nie przekonać się na własnej skórze, że zagrożenie jest realne, należy ciągle poszerzać i doskonalić procedury bezpieczeństwa.

### Człowiek – najsłabszy punkt systemu

Świadomość istnienia zagrożeń na poziomie pracownika jest równie ważna co na poziomie całej organizacji. To konkretna osoba ma dostęp do informacji i pomimo obowiązującej ją umowy, zapisów o poufności i kar grożących za złamanie tajemnicy, a także jej dobrych intencji i zaufania, dane mogą wypłynąć z firmy.

Nierzadko podczas budowy systemów obronnych wysiłek zespołu skupia się na tworzeniu zaawansowanych systemów kontroli dostępu, antywirusów i firewalli. Pomijany jest natomiast czynnik ludzki. Atakujący często uderzają w najsłabszy element systemu, czyli człowieka, stosując zaawansowane socjotechniki. Najsłynniejszy haker XX wieku, Kevin Mitnick, sam o sobie pisze: „łamałem ludzi, nie hasła”.

Atrybutem napastnika często jest jedynie telefon. Brak kontaktu wzrokowego pozwala mu podszyć się pod dowolną osobę (szefa, kuriera albo klienta). Dlatego tak ważne jest, aby pracownicy wiedzieli, jakich informacji mogą udzielać, a które bezwzględnie są zastrzeżone, jak również by byli przygotowani i zaznajomieni z technikami, które może wykorzystał napastnik.

Dzięki dużym umiejętnościom interpersonalnym i – co może wydać się zaskakujące – również aktorskim haker szybko zdobywa zaufanie oraz buduje więź emocjonalną z ofiarą, a pod przykrywką niewinnego pytania potrafi wyciągnąć, często niezauważenie, ważne informacje.

Wykrycie takiego socjoataku może być bardzo trudne – rozmowa telefoniczna przypomina zwykły kontakt handlowy, a do tego atak może składać się z serii rozmów rozłożonych w czasie, podczas których napastnik wyciąga pojedyncze informacje. „Najlepsi” – podszywając się np. pod menedżera z innego działu – potrafią uzyskać hasło do systemu lub przesłać dane na wskazany adres.

### Jak się bronić?

Obroną przed tego typu atakami jest zwiększanie świadomości pracowników poprzez wspomniane na początku procedury i budowanie systemów bezpieczeństwa. Jednak w przypadku ludzi dochodzi jeszcze pewien aspekt psychologiczny. O ile do narzędzia informatycznego można wgrać aktualizacje i być pewnym, że system zadziała i zawsze będzie działać, o tyle w przypadku ludzi już tak nie jest.

Człowiek dąży do ułatwiania sobie życia (co w większości przypadków jest zaletą), a wywiązywanie się z procedur zwykle wymaga dodatkowych nakładów czasu i pracy. Dodatkowo, w miarę uzyskiwania większej pewności i rutyny, zmniejsza się poczucie zagrożenia. Wówczas łatwiej o pójście drogą na skróty, z pominięciem uciążliwych procedur.

#### Jedenaście obszarów mających wpływ na bezpieczeństwo informacji w organizacji według normy ISO/IEC 27001

- Polityka bezpieczeństwa
- Organizacja bezpieczeństwa informacji
- Zarządzanie aktywami
- Bezpieczeństwo zasobów ludzkich
- Bezpieczeństwo fizyczne i środowiskowe
- Zarządzanie systemami i sieciami
- Kontrola dostępu
- Zarządzanie ciągłością działania
- Pozyskiwanie, rozwój i utrzymanie systemów informatycznych
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- Zgodność z wymaganiami prawnymi i własnymi standardami

By nie dopuścić do uśpienia czujności pracowników, trzeba nieustannie monitorować i doskonalić ich wiedzę poprzez szkolenia z zakresu potencjalnych źródeł ataku, socjotechnik oraz zabezpieczeń i procedur. Konieczne są też okresowe audyty sprawdzające świadomość zagrożeń oraz praktyczne wykorzystanie tej wiedzy i jednocześnie przypominające o istocie jej stosowania.

### Sieci i systemy informacyjne

Jakość infrastruktury sieciowej i wykorzystywanych systemów są kolejnymi elementami świadczącymi o poziomie bezpieczeństwa informacji w przedsiębiorstwie. Charakterystyczną cechą świata IT jest ciągła i szybka zmiana. Bardzo często pojawiają się nowe rozwiązania, kolejne wersje, ulepszenia oraz... luki w systemie i nowe zagrożenia.

#### Bezpieczeństwo informacji w ofercie BCC

BCC oferuje usługi związane z wdrażaniem systemów zarządzania bezpieczeństwem informacji i przygotowaniem do certyfikacji na zgodność z normą ISO/IEC 27001. Realizuje projekty doradcze w zakresie: zarządzania ciągłością działania (ang. Business Continuity Management), zarządzania ryzykiem operacyjnym i procesami biznesowymi.

Adresatem usługi są duże firmy i organizacje posiadające złożoną infrastrukturę IT, zorientowane na optymalizację zarządzania usługami i zasobami IT.

Konsultanci BCC specjalizują się w opracowaniu strategii zarządzania działami IT na zgodności z systemami zarządzania usługami IT ISO/IEC 20000 i ITIL v3.

W ramach audytów bezpieczeństwa IT BCC weryfikuje funkcjonujące w firmie procedury, bada systemy produkcyjne, serwisy WWW, bazy danych, jak również analizuje i sprawdza strukturę sieciową wraz z urządzeniami (switch, firewall itp). Dopelnieniem audytu są testy penetracyjne, które sprawdzają funkcjonowanie zabezpieczeń w rzeczywistych okolicznościach. Wyniki audytu są przedstawiane w formie raportu, który odzwierciedla stan bezpieczeństwa informacji w przedsiębiorstwie. Wskazuje zarówno na elementy krytyczne, które stanowią bezpośrednie zagrożenie, jak również zawiera rekomendacje dotyczące procesów i działań, które warto w firmie zaimplementować.

Dobry administrator musi na bieżąco monitorować aktualne wersje oprogramowania znajdującego się w przedsiębiorstwie, zwłaszcza że zmiany w firmowej sieci i systemach zachodzą równie często. Niejednokrotnie zmiany te prowadzą do powstania luk bezpieczeństwa oraz niespójności konfiguracyjnych w infrastrukturze IT. A to z kolei może być bezwzględnie wykorzystane przez napastnika.

Na początku zobaczmy, jakimi technikami może się posłużyć haker. Poniżej przedstawię trzy podstawowe metody ataków.

Najprostsze, lecz pozwalające na szybkie uzyskanie pełnej kontroli nad atakowanym obiektem, jest użycie exploitów. Exploity to łatwo dostępne w Internecie aplikacje, które wykorzystują zazwyczaj ogólnie znane błędy w aplikacjach lub serwerze, np. przepełnienie bufora (ang. Buffer Overflow). To pozwala na uruchomienie dowolnej aplikacji na serwerze lub uzyskanie dostępu do konta administratora.

Drugą, bardziej zaawansowaną metodą, są próby uzyskania nieautoryzowanego uwierzytelnienia w systemie poprzez podszycie się pod rzeczywistego użytkownika. Jest wiele sposobów na uzyskanie hasła użytkownika, poczynając od już wcześniej wspomnianych socjotechnik, poprzez próby ataków siłowych i słownikowych oraz podsłuchu sieciowego.

Sprawny haker zawsze sprawdzi, czy w ruchu sieciowym nie krążą hasła w otwartym tekście lub czy może ich szyfrowanie jest na tyle słabe, że da się szybko złamać. Przykładem niewystarczającego szyfrowania może być sieć bezprzewodowa zabezpieczona kluczem WEP.

Ostatecznie napastnik może posłużyć się techniką Man In the Middle i stać się niejako serwerem Proxy pomiędzy systemem a użytkownikiem, a następnie po wylogowaniu użytkownika korzystać dalej z jego sesji.

Zdarzają się także ataki typu DoS, których celem nie jest uzyskanie dostępu do usługi, ale uniemożliwienie jej funkcjonowania. Klasyczny atak tego typu polega na wysłaniu dużej liczby spreparowanych komunikatów, tak aby atakowany system nie mógł wykonywać swoich normalnych czynności, a jedynie zajmował się odpowiedziami na bezwartościowe komunikaty wysyłane przez atakującego.

### Testy bezpieczeństwa systemów IT

- Black Box – osoby testujące nie posiadają wiedzy lub posiadają minimalną wiedzę na temat atakowanego celu. Testy te są najbardziej zbliżone do rzeczywistych zagrożeń, jednak wiążą się z dużo dłuższym czasem trwania testów.
- Cristal Box – osoby testujące mają bardzo szczegółową wiedzę na temat systemu; testy są wówczas bardziej symulacją, jednak pozwalają dokładnie sprawdzić dany element, co znacznie oszczędza czas.
- Gray Box – jest to połączenie dwóch powyższych rodzajów testów, osoby testujące otrzymują pewną ograniczoną liczbę informacji.

### Audyt bezpieczeństwa IT

Obroną przez tego typu zagrożeniami infrastruktury IT jest systematyczność. Dotyczy to zarówno bieżącego utrzymania infrastruktury poprzez cykliczne aktualizacje, jak również poprzez okresowe audyty bezpieczeństwa systemów. Takie audyty mogą być przeprowadzane przez pracowników, czyli administratorów, lub osoby z zewnątrz. W przypadku skorzystania z usług firmy zewnętrznej ważne jest ustalenie, jaki zakres informacji o systemach zostanie przekazany audytorom.

Warto co jakiś czas poddać się sprawdzeniu przez wyspecjalizowaną i doświadczoną firmę zewnętrzną, której pracownicy są zaznajomieni ze słabymi punktami w najbardziej aktualnych wersjach aplikacji i systemów oraz posiadają wiedzę o najnowszych zabezpieczeniach i sposobach radzenia sobie z atakami.

Podczas audytu badane są poszczególne segmenty infrastruktury IT, takie jak topologia sieci, reguły firewalla i inne urządzenia sieciowe, bazy danych oraz systemy produktywne pod kątem bezpieczeństwa. W dalszej kolejności należy sprawdzić system zarządzania kontami użytkowników, sposoby logowania do systemów oraz mechanizmy i ustalenia dotyczące polityki zarządzania hasłami.

Warto podsłuchać, co tak naprawdę dzieje się w naszej sieci lokalnej, i przeanalizować ruch pomiędzy kluczowymi punktami infrastruktury.

Ostatnim elementem audytu jest sprawdzenie, jak działa system zarządzania kopiami zapasowymi oraz plany ciągłości działań systemów produktywnych.

Audyt bezpieczeństwa powinien dawać kompleksową informację zwrotną o poziomie bezpieczeństwa IT w przedsiębiorstwie. Jego efektem jest zwykle także lista zadań korygujących, które pozwolą na ograniczenie ryzyka nieautoryzowanego wypływu ważnych informacji.

Kolejnym krokiem w audytach bezpieczeństwa mogą być testy penetracyjne, podczas których audytor wciela się w rolę hakera i przeprowadza symulowany atak w celu sprawdzenia podatności zabezpieczeń. Taki test jest rzeczywistym atakiem i może spowodować uszkodzenie systemu bądź niedostępność usługi. Dlatego warto się zastanowić, czy takie działania przeprowadzać na systemach produktywnych, czy może przygotować dedykowane środowisko testowe, będące zarazem kopią fragmentu sieci bądź systemu.

Ważną decyzją, którą należy podjąć, jest wybór rodzaju testów. W zależności od tego, czy mają to być testy Black, Cristal czy Gray, testerom są przekazywane określone informacje.

Pojęcie bezpieczeństwa informacji jest szerokie i łączy się w nim wiele elementów. Cały system jest na tyle bezpieczny, na ile jest bezpieczne jego najsłabsze ogniwo. To te najmniej chronione miejsca, luki w systemie są najbardziej narażone na ataki. Dlatego warto kwestię bezpieczeństwa informacji rozpatrywać całościowo i dbać o nie w szerokim kontekście.



Autor:

Dariusz Izidor  
BCC