Informatyka Śledcza jako narzędzie zabezpieczania i analizy wrażliwych danych

Daniel Suchocki
Dyrektor Generalny

Maciej Karmoliński
Dyrektor Operacyjny

FOR SEC
Forensics&Security

1. Przepisy i procedury

FOR SEC
Forensics&Security

Incydenty naruszenia bezpieczeństwa IT

Zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych takie jak

- przypadki naruszenia poufności (ujawnienie niepowołanym osobom)
- niedostępność oraz działania niezgodne ze specyfikacją (błędne) systemów informatycznych
- infekcje, propagacja i działanie szkodliwego oprogramowania
- rozpoznanie, penetracja i próby omijania systemów zabezpieczeń;
- niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych;
- ataki odmowy usługi na systemy informatyczne;

FOR SEC
Forensics&Security

Incydenty naruszenia bezpieczeństwa IT

- ataki nieautoryzowanego dostępu do aplikacji,
- kradzież lub zniszczenie urządzeń przetwarzających lub/i przechowujących informacje oraz nośników danych;
- wyłudzenia (lub próby wyłudzeń) informacji wrażliwych
- ataki socjotechniczne, ataki z wykorzystaniem phishing'u, skimming'u oraz innych technik zagrażających naruszeniu poufności, dostępności i integralności informacji;
- incydenty wielokomponentowe (złożone incydenty dotyczące wielu systemów, wykorzystujące wiele wektorów ataków itp.);

FOR SEC
Forensics&Security

Incydenty naruszenia bezpieczeństwa IT

Czy mają Państwo instrukcję działania na incydenty naruszenia bezpieczeństwa IT?

Czy korzystają Państwo z zewnętrznej firmy obsługującej Państwa w przypadku wystąpienia incydentów?

Jaki jest czas reakcji tej firmy?

FOR SEC
Forensics&Security

Testy penetracyjne

Testy penetracyjne, nazywane również pentestami, to **kontrolowane ataki hackerskie** na aplikację, stronę, system informatyczny lub sieć klienta.

Podczas ataku specjaliści oceniają poziom bezpieczeństwa, wykrywają aktualne luki i sugerują metody naprawy błędów i defektów. Dzięki temu przedsiębiorcy są w stanie ochronić się na przykład przed wyciekiem danych swoich klientów i pracowników lub zapobiec przejęciu systemu przez hakerów.

FOR SEC
Forensics&Security

Testy penetracyjne

Czy realizują Państwo testy penetracyjne dla najbardziej istotnych systemów?

FOR SEC
Forensics&Security

Aktualizacja oprogramowania

Przeciętny użytkownik Windowsa wie, że jest to platforma narażona na ataki szkodliwych programów różnego typu.

Zwiększa się też liczba zagrożeń atakujących inne systemy operacyjne. Nawet laicy zabezpieczają dziś swoje komputery i smartfony za pomocą rozwiązań typu Internet Security z automatycznie aktualizowaną bazą wirusów.

Wielu nie zdaje sobie jednak sprawy z konieczności regularnego aktualizowania systemu operacyjnego i zainstalowanego na nim oprogramowania czy aplikacji, a w szczególności przeglądarek internetowych.

FOR SEC
Forensics&Security

Aktualizacja oprogramowania

Czy dbają Państwo o aktualizację oprogramowania?

FOR SEC
Forensics&Security

Polityka zarządzania bezpieczeństwem haseł

Jednym z elementów systemu bezpieczeństwa jest kontrola dostępu do zasobów komputerowych.

Wśród wielu metod najpopularniejszą jest kontrola dostępu za pomocą **haseł**.

W związku z tym istotnego znaczenia nabiera **polityka zarządzania hasłami**, wymuszająca zarówno działania organizacyjne, jak i zachowania użytkowników korzystających z tej metody kontroli dostępu.

FOR SEC
Forensics&Security

Polityka zarządzania bezpieczeństwem haseł

Czy mają Państwo politykę zarządzania bezpieczeństwem haseł w firmie?

FOR SEC
Forensics&Security

2. Ochrona danych

FOR SEC
Forensics&Security

Uszkodzenie dysku twardego lub przypadkowe usunięcie danych

Jeżeli dysk uległ uszkodzeniu podczas pracy, to pierwszą rzeczą, jaką bezwzględnie trzeba zrobić, jest **odłączenie go od źródła zasilania**.

W przypadku, gdy dysk został uszkodzony poza komputerem nie należy go podłączać do komputera ani próbować w jakikolwiek sposób sprawdzać, czy działa.

Upadek w większości przypadków skutkuje awarią dysku, tak więc jeśli znajdują się na nim ważne dane, najlepszym wyjściem jest **powierzenie ich odzyskania wykwalifikowanym specjalistom**.

FOR SEC
Forensics&Security

Uszkodzenie dysku twardego lub przypadkowe usunięcie danych

Czy wiedzą Państwo, co zrobić w przypadku uszkodzenia dysku twardego z komputera bądź przypadkowego usunięcia danych z dysku?

FOR SEC
Forensics&Security

Mechanizmy blokujące dostęp do danych na urządzeniach mobilnych

Aby uniemożliwić osobom niepowołanym dostęp do urządzenia mobilnego pierwszym krokiem jest zabezpieczenie go **kodem dostępu** – tzw. PIN

A co w momencie kiedy złodziej dostanie się do zawartości naszego smartfona? Możemy mu wówczas uniemożliwić pobranie danych poprzez ich wcześniejsze **zaszyfrowanie**. Zazwyczaj wymaga to tylko włączenia odpowiednich funkcji lub zainstalowania programu szyfrującego.

Uwaga! W ten sposób możemy zaszyfrować tylko dane przechowywane w pamięci urządzenia. Pliki zapisane na kartach pamięci możemy zabezpieczyć, używając któregoś z wielu dostępnych programów czy aplikacji.

FOR SEC
Forensics&Security

Mechanizmy blokujące dostęp do danych na urządzeniach mobilnych

Czy mają Państwo mechanizmy (np. PIN lub szyfrowanie dysku) blokujące dostęp do danych na urządzeniu mobilnym po jego utracie?

FOR SEC
Forensics&Security

Zdalne usuwanie danych z urządzeń mobilnych

Zainstalowanie odpowiedniej aplikacji pozwala na **zdalny dostęp** do urządzenia mobilnego za pomocą przeglądarki internetowej i **trwałe usunięcie danych**.

FOR SEC
Forensics&Security

Zdalne usuwanie danych z urządzeń mobilnych

Czy mają Państwo możliwość zdalnego, trwałego usunięcia danych z urządzenia mobilnego?

FOR SEC
Forensics&Security

3. Pracownicy

FOR SEC
Forensics&Security

Bezpieczeństwo firmy zależy od jej pracowników

Nieodpowiedzialne działania nieprzeszkolonych pracowników niższego i średniego szczebla mogą spowodować, że do sieci wewnętrznej przedsiębiorstwa przedostanie się wrogie oprogramowanie, co może doprowadzić do ataku na stronę internetową firmy, ingerencję w bazę klientów, czy nawet do ataku na konto bankowe firmy.

Każdy z pracowników powinien być świadom zagrożeń jakie czyhają na niego w sieci oraz jakie mogą być ich konsekwencje.

FOR SEC
Forensics&Security

Bezpieczeństwo firmy zależy od jej pracowników

Czy pracownicy firmy są przeszkoleni w obszarze bezpieczeństwa IT?

Czy pracownicy podpisywali oświadczenie, że odbyli takie szkolenie i są świadomi potencjalnych zagrożeń?

FOR SEC
Forensics&Security

Wykorzystywanie własnego sprzętu w celach służbowych

Od jakiegoś czas **BYOD**, czyli „Bring Your Own Device” to trend, który utrzymuje się w biznesie. O ile przynosi wiele korzyści w postaci oszczędności oraz bardziej przyjaznych narzędzi pracy, które wybierają sami użytkownicy i które pozwalają im na zdalny dostęp do służbowych plików, to jednak wymaga przygotowania organizacji i zapewnienia odpowiednich procedur bezpieczeństwa.

Jednym z największych niebezpieczeństw jest **integracja prywatnego urządzenia z firmową siecią**. W przypadku włamania się do źle zabezpieczonego prywatnego sprzętu osoby niepowołane mogą otrzymać dostęp do naszych wrażliwych danych.

FOR SEC
Forensics&Security

Wykorzystywanie własnego sprzętu w celach służbowych

Czy pracownicy mogą używać prywatnego sprzętu – komputera, telefonu – do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych?

Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, pendrive) do infrastruktury służbowej?

FOR SEC
Forensics&Security

Dane ze sprzętów służbowych pracownika

Przekazanie pracownikowi komputera, podobnie jak każdego innego narzędzia pracy, służy realizacji celów zakładanych przez pracodawcę. Z tego powodu ma on niczym nieograniczone prawo kształtowania zasad wykorzystania przez pracownika tego narzędzia.

Oczywiście integralną częścią komputera są **dokumenty służbowe** przechowywane i tworzone w jego pamięci. Podwładny powinien nie tylko dbać o ich bezpieczeństwo, ale także nie ma prawa ich swobodnego usuwania.

FOR SEC
Forensics&Security

Dane ze sprzętów służbowych byłego pracownika

Każdy pracownik, którego stosunek pracy ustał powinien **rozliczyć się ze sprzętu służbowego**, oddać komputer i telefon służbowy wraz z jego zawartością – dokumentami oraz kontaktami.

Zazwyczaj sprzęt po byłym pracowniku jest przywracany do ustawień fabrycznych i przekazywany nowemu pracownikowi.

FOR SEC
Forensics&Security

Dane ze sprzętów służbowych byłego pracownika

Przed przywróceniem sprzętu do ustawień fabrycznych pracodawca powinien **zabezpieczyć (zgrać) wszystkie dane**, które znajdują się na komputerze i telefonie. Może zrobić to sam za pomocą specjalistycznego oprogramowania lub zwrócić się do firmy, które specjalizują się w tego typu zadaniach.

Dzięki temu pracodawca będzie miał w każdej chwili dostęp do wszystkich danych byłego pracownika.

FOR SEC
Forensics&Security

Dane ze sprzętów służbowych byłego pracownika

Czy zabezpieczają Państwo dane z telefonów i komputerów służbowych pracowników odchodzących z Państwa firmy?

FOR SEC
Forensics&Security