Sąd Rejonowy Lublin-Wschód w Lublinie z siedzibą w Świdniku

Cyberbezpieczeństwo

Uwaga

W związku ze wzmożonymi próbami ataków cybernetycznych polegających na podszywaniu się pod m.in. pomoc techniczną banków z prośbą o instalowanie oprogramowania Quick Support (Team Viewer), AnyDesk na smartfonach lub komputerach PC lub innych aplikacji pozwalających na przejęcie władzy nad urządzeniem w tak zwanej "sesji nagrywanej" prosimy o szczególną czujność i uwagę w sutuacjach zaprezentowanych w nagraniu (link do YouTube poniżej) oraz na stronie niebezpiecznik.pl.

https://www.youtube.com/watch?v=SbCcmLqmQSs

https://niebezpiecznik.pl/post/zlodziej-falszywy-pracownik-banku-rozmowa/

Podstawowe zasady bezpiecznego poruszania się w cyberprzestrzeni

• Zawsze stosuj sprawdzone oprogramowanie przeciw wirusom i spyware, najlepiej z funkcjonalnością firewalla,
• Przeprowadzaj regularne aktualizacje oprogramowania oraz baz danych wirusów,
• Nie otwieraj plików nieznanego pochodzenia,
• Zawsze skanuj pobrane pliku z Internetu za pomocą programu antywirusowego,
• Regularnie skanuj swój komputer oprogramowaniem antywirusowym,
• Nie podawaj swoich danych osobowych, informacji dot. Kart płatniczych na niezweryfikowanych stronach, które nie zbudzają twojego zaufania,
• Przed wysłaniem w wiadomości swoich danych poufnych, pamiętaj o ich zaszyfrowaniu,
• Pamiętaj, że żaden bank nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji,
• Nie podłączaj do komputera nośników (pendrive, płyty DVD, CD i inne) niewiadomego pochodzenia,
• Stosuj tzw. mocne hasła, składające się z co najmniej 12 znaków, zawierające cyfry, wielkie oraz małe litery, znaki specjalne.
• Pamiętaj aby stosować różne hasła do różnych usług oraz aplikacji,
• Unikaj korzystania z publicznych dostępów Wi-Fi, a w szczególności nie korzystaj z nich przy realizacji transakcji finansowych.

Jak się ustrzec przed cyberzagrożeniami oraz sposoby obrony przed nimi

1. Ataki wymierzone w urządzenia sieciowe

W gospodarstwie domowym oraz w firmie istnieje wiele urządzeń sieciowych takich jak Smart TV, urządzenia przenośne, urządzenia Smart House oraz wiele innych. Z uwagi na fakt, że urządzenia są dość słabo zabezpieczone oraz brak w nich aktualizacji oprogramowania, stanowią one łatwy łup dla cyberprzestępców.

Jak się ochronić? Najłatwiejsze sposoby:

- regularna aktualizacja oprogramowania we wszystkich urządzeniach połączonych z Internetem,
- ograniczenie dostępu do Internetu urządzeniom, które tego nie potrzebują,
- stosowanie zabezpieczeń infrastruktury dostępowej,
- bieżące monitorowanie infrastruktury.

Zalecane jest też wydzielanie segmentów sieci, w której działają potencjalnie zagrożone urządzenia i eliminacja zbędnej komunikacji z Internetem. Jeśli urządzenia – np. czujniki stanowiące element infrastruktury IoT – wymagają dostępu do sieci zewnętrznej, wówczas niezbędne jest przeprowadzenie testów zabezpieczeń konkretnych urządzeń i infrastruktury, której są częścią.

2. Ransomware

Istotą tego zagrożenia jest zaszyfrowanie danych użytkownika przez złośliwe oprogramowanie (np. na jego komputerze PC), a następnie żądanie okupu za odszyfrowanie danych.

Jak się ochronić? Najłatwiejsze sposoby:

- regularne tworzenie kopii bezpieczeństwa danych na nośnikach przechowywanych w bezpiecznym miejscu (także w zewnętrznych centrach danych) i zapewnienie szybkiego przywrócenia danych,
- zabezpieczanie systemami antywirusowymi urządzeń komputerowych,
- uczestnictwo w szkoleniach budujących świadomość zagrożeń w sieci i sposobów postępowania z nimi.

Zalecane jest aby uchronić się przed atakami ransomware przydatne będą narzędzia kontrolujące funkcjonowanie brzegu sieci i poszczególnych komputerów. Dzięki temu realne staje się wykrycie złośliwego kodu szyfrującego jeszcze zanim zablokowany zostanie dostęp do najbardziej newralgicznych danych. W roli dodatkowych zabezpieczeń sprawdza się oprogramowanie ochronne dla stacji roboczych i serwerów.

3. Ataki wykorzystujące luki w oprogramowaniu oraz platformach

internetowych

Infrastruktura sieciowa i środowiska IT składają się z coraz większej ilości rozwiązań, standardów, platform, usług i protokołów sieciowych. Cyberprzestępcy stawiają coraz większy nacisk na wyszukiwanie podatności istniejących we wszystkich - dostępnych z poziomu Internetu - elementach infrastruktury. Wykryte luki mogą zostać wykorzystane do przeprowadzenia ataku.

Jak się ochronić? Najłatwiejsze sposoby:

- polityka aktualizacji oprogramowania (także wbudowanego w urządzenia sieciowe),
- systematyczna modernizacja platform aplikacyjnych,
- dobre praktyki tworzenia kodu,
- wykorzystanie dodatkowych usług, oferowanych przez operatorów, np. WAF (Web Application Firewall).

Zalecane jest aby zminimalizować podatności należy separować infrastruktury krytycznej od sieci Internet oraz ograniczenie ilości rozwiązań dostępnych z jej poziomu. Warto również dokonać oceny poziomu bezpieczeństwa infrastruktury sieciowej. W tym obszarze pomocne są m.in. testy penetracyjne. Aby ograniczyć ryzyko związane z wykorzystaniem podatności w platformach internetowych warto użyć firewalla aplikacyjnego (WAF), który ukierunkowany jest na wykrywanie ataków i ochronę aplikacji w wyższych warstwach komunikacji.

4. Rozproszone ataki DDoS

Celem ataków DDoS jest doporowadzenie do sytuacji, w której konkretne usługi obecne w Internecie będą niedostępne, a sam atak – chociażby z tytułu rozproszenia – będzie trudny do zablokowania.

Jak się ochronić? Najłatwiejsze sposoby:

- monitorowanie sprawności infrastruktury,
- wykorzystywanie usług ochrony przed atakami na poziomie ISP,
- zapewnienie nadmiarowości infrastruktury (np. u partnera zewnętrznego czy za pośrednictwem modelu cloud) wraz z możliwością łatwego przełączenia się,
- prewencyjne wykorzystanie rozwiązań odseparowujących ruch DDoS lub wdrożenie usług dostawcy Internetu.

Zalecane jest wsparcie ze strony dostawcy usług infrastrukturalnych, w tym dostawcy Internetu. Dobrą praktyką jest wcześniejsze przeanalizowanie infrastruktury pod kątem wykrycia newralgicznych punktów i tzw. „najsłabszych ogniw”. Ważne jest także wdrożenie systemów monitoringu infrastruktury na potrzeby wczesnego wykrywania ataków DDoS oraz zapewnienie jak najwyższej skalowalności środowiska sieciowo-

aplikacyjnego. Działaniem prewencyjnym może być też wykorzystanie specjalistycznych rozwiązań, które mogą odseparować ruch związany z trwającym atakiem DDoS.

5. Phishing

Ataki phishingowe mają na celu podszycie się pod znaną markę, osobę (np. bank) aby uzyskać dostęp do twoich wrażliwych danych. Najczęściej wykorzystywane są do tego maile, ale widać wzrost phishingu za pośrednictwem portali społecznościowych i komunikatorów.

Jak się ochronić? Najłatwiejsze sposoby:

- instalacja oraz regularna aktualizacja oprogramowania antywirusowego, które ułatwia weryfikację poprawności wiadomości,
- weryfikowanie nadawców komunikatów,
- monitorowanie infrastruktury,
- uczestnictwo w szkoleniach i budowanie dobrych nawyków.

Zalecane jest wprowadzenie do polityki postępowania w najbardziej newralgicznych obszarach – jak akceptacja wydatków, przekazywanie danych dostępowych, czy praca z załącznikami. W ograniczeniu skutków ewentualnego ataku phishingowego pomocne okazują się narzędzia utrudniające przestępcom zainstalowanie szkodliwego oprogramowania, uniemożliwiające także wykorzystanie skradzionych danych. W wykrywaniu bardziej złożonych ataków, których phishing jest tylko jednym z etapów, niezbędne okazują się rozwiązania do bieżącego monitorowania działania infrastruktury IT.

6. Precyzyjnie ukierunkowane ataki typu advanced persistent threat (apt)

Ataki APT są oparte na połączeniu wielu wektorów i metod ataku, często rozłożonych w czasie i precyzyjnie ukierunkowanych na określoną organizację i cel. Z tego powodu bywają niewykryte przez wiele miesięcy. Ataki APT poprzedzone są analizą słabych punktów organizacji. Obok luk bezpieczeństwa, błędów w oprogramowaniu i rozproszonych ataków dużej skali zastosowanie znajdują narzędzia socjotechniczne mające na celu skłonić pracowników do podjęcia określonego działania.

Jak się ochronić? Najłatwiejsze sposoby:

- monitorowanie i wykrywanie anomalii funkcjonowania środowisk IT w firmie – od warstwy sieciowej, po zachowania użytkowników,
- korelacja trendów,
- budowanie świadomości zagrożeń wśród użytkowników.

Wykrycie ataków APT powinno być wparte także specjalistycznymi narzędziami. Wśród nich warto wskazać m.in. rozwiązania behawioralne, które są w stanie wykrywać anomalnie w funkcjonowaniu sieci oraz działaniu użytkowników, a także systemy

bezpieczeństwa wykorzystujące funkcje analityczne w celu korelacji wykrywanych zdarzeń i trendów pod kątem występowania zagrożeń. Dobrą praktyką jest też separacja obowiązków, tak, aby pracownicy mieli dostęp tylko do narzędzi potrzebnych im w pracy. Przydatne okazuje się też oddzielenie najbardziej newralgicznych obszarów sieci od infrastruktury Internetu. W przypadku złożonych, długotrwałych i rozproszonych ataków APT bezcenna nierzadko okazuje się też ludzka intuicja. Dlatego tak ważne jest posiadanie doświadczonego zespołu administratorów. W firmach, dla których pozyskanie tego typu kompetencji w ramach lokalnego zespołu IT jest niemożliwe, przydatne okazuje się wykorzystanie zewnętrznych usług świadczonych m.in. przez operatorów.

Metadane

Data publikacji : 31.03.2021
Data modyfikacji : 14.06.2021
Rejestr zmian

Podmiot udostępniający informację:
Sąd Rejonowy Lublin-Wschód w Lublinie z siedzibą w Świdniku

Osoba wytwarzająca/odpowiadająca za informację:
Rafał Nowosacki Oddział Informatyczny

Osoba udostępniająca informację:
Rafał Nowosacki Oddział Informatyczny

Osoba modyfikująca informację:
Rafał Nowosacki