PORADNIK – PRCyber-03
Cyberbezpieczeństwo – Jak zapobiegać atakom typu ransomware?

(Wydanie 1 – lipiec 2020 r.)

Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Nie ma sposobu, aby całkowicie zabezpieczyć swoją organizację przed infekcją szkodliwym oprogramowaniem. Z tego powodu należy zastosować podejście „wielowarstwowej obrony". Oznacza to stosowanie **warstw obrony z kilkoma ograniczeniami na każdej warstwie**. Będzie wówczas więcej możliwości wykrycia szkodliwego oprogramowania a następnie zatrzymania go, zanim wyrządzi prawdziwą szkodę Twojej organizacji. Należy przyjąć, że niektóre rodzaje szkodliwego oprogramowania będą infiltrować organizację, więc należy podjąć kroki w celu ograniczenia wpływu takiego działania i przyspieszenia reakcji na zagrożenie.

Poniżej znajdziesz 4 wskazówki, jak możesz zabezpieczać swoją organizację.

Wskazówka 1: rób regularne kopie zapasowe

- Kluczowym działaniem jest zapewnienie aktualnych kopii zapasowych systemów oraz ważnych plików - jeśli tak zrobisz, będziesz mógł odzyskać swoje dane bez konieczności płacenia okupu.
- Wykonuj regularne kopie zapasowe najważniejszych plików – sposoby mogą być rożne, zależne od typów danych i organizacji - sprawdź, czy wiesz, jak przywrócić pliki z kopii zapasowej.
- Upewnij się, że kopia zapasowa jest przechowywana poza Twoją siecią („offline"), w pamięci masowej nie podłączonej do Twojej sieci lub w dedykowanej do tego celu usłudze chmurowej.
- Usługi synchronizacji w chmurze (takie jak Dropbox – usługa przestrzeni dyskowej świadczona przez firmę Dropbox, OneDrive – wirtualny dysk oferowany przez Microsoft, SharePoint – platformę aplikacji webowych firmy Microsoft lub Dysk Google - usługę do przechowywania i synchronizacji plików stworzona przez firmę Google) nie powinny być używane jako jedyna kopia zapasowa. Wynika to z faktu, że mogą one automatycznie zostać zsynchronizowane natychmiast po „zaatakowaniu plików", a wówczas utracisz również połączone kopie.
- Upewnij się, że urządzenie zawierające kopię zapasową (takie jak zewnętrzny dysk twardy lub pamięć USB) nie jest na stałe podłączone do sieci i najlepiej, aby kopii zapasowych było kilka. Atakujący może zdecydować się na atak ransomware, gdy wie, że nośnik danych zawierający kopie zapasowe jest podłączony do sieci.

Wskazówka 2: Zapobiegaj przedostawaniu się szkodliwego oprogramowania na urządzenia

Możesz zredukować ryzyko przedostania się do sieci w Twojej organizacji szkodliwych zawartości poprzez zastosowanie następujących działań:

- filtrowanie plików, zezwolenie na odbieranie plików określonych typów;

- blokowanie witryn, o których wiadomo, że są szkodliwe – możesz skorzystać z informacji dostępnych na stronie https://www.cert.pl/news/single/ostrzezenia_phishing/
- aktywne sprawdzanie zawartości stron internetowych, wiadomości e-mail itp.,
- korzystanie z programów antywirusowych, które potrafią blokować znane im szkodliwe oprogramowanie na podstawie dostępnych sygnatur wirusów.

Zazwyczaj są one wykonywane przez usługi sieciowe, a nie urządzenia użytkowników, przykładowo:

- filtrowanie poczty (w połączeniu z filtrowaniem spamu), które może blokować szkodliwe wiadomości e-mail i usuwać z nich wykonywalne załączniki;
- filtrowanie z wykorzystaniem serwerów proxy, które blokują dostęp do znanych szkodliwych stron internetowych;
- bramy bezpieczeństwa internetowego, które mogą sprawdzać zawartość niektórych protokołów pod kątem znanego szkodliwego oprogramowania;
- bezpieczne listy przeglądania w przeglądarkach internetowych, które mogą uniemożliwić dostęp do witryn znanych z dystrybucji szkodliwych zawartości.

Niektóre ataki ransomware są przeprowadzane przez atakujących, którzy uzyskali dostęp do sieci za pomocą protokołu zdalnego dostępu, takiego jak RDP (ang. *Remote Desktop Protocol*). Powinieneś uniemożliwić dostęp do Twoich sieci przestępcom stosujących tzw. atak typu „Brute-Force", czyli opartego na metodzie prób i błędów. Możesz to zrobić wdrażając w organizacji m.in. uwierzytelnianie wieloskładnikowe (MFA), czy stosując połączenia wykorzystujące wirtualną sieć prywatną (VPN).

Wskazówka 3: Zapobiegaj uruchamianiu szkodliwego oprogramowania na urządzeniach

Podejście „wielowarstwowej ochrony" zakłada, że przestępca może znaleźć „lukę" w zabezpieczeniach i szkodliwe oprogramowanie może dotrzeć do Twoich urządzeń. Dlatego powinieneś podjąć kroki, aby zapobiec uruchomieniu szkodliwego oprogramowania w sytuacji gdy, mimo wszystko, znajdzie się w Twojej organizacji. Wymagane kroki będą się różnić dla każdego typu urządzenia i systemu operacyjnego, ogólnie jednak należy rozważyć użycie zabezpieczeń na poziomie urządzenia, takich jak:

1. Centralne zarządzanie urządzeniami korporacyjnymi w celu:
    - zezwolenia tylko zaufanym aplikacjom na działanie na urządzeniach firmy poprzez wykorzystanie dedykowanych rozwiązań, w tym funkcji AppLocker;
    - zezwolenia na uruchamianie aplikacji tylko z zaufanych sklepów z aplikacjami (lub innych zaufanych lokalizacji).

2. Korzystanie z wersji *Enterprise* oprogramowania antywirusowego. Aktualizuj na bieżąco oprogramowanie wraz z jego bazą wirusów. Zapewnij swoim pracownikom edukację w zakresie bezpieczeństwa i szkolenia uświadamiające.
3. Wyłącz lub ogranicz makra w pakietach biurowych, co oznacza:
    - wyłączanie (lub ograniczanie) innych środowisk skryptowych (np. PowerShell);
    - wyłączenie uruchamiania automatycznego dla podłączonych nośników (lub uniemożliwienie korzystanie z nośników wymiennych, jeśli nie jest to wymagane);
    - ochronę swoich systemów przed możliwymi szkodliwymi makrami w Microsoft Office.

Ponadto atakujący może wymusić wykonanie kodu, wykorzystując luki w zabezpieczeniach urządzenia. Zapobiegaj temu, utrzymując urządzenia poprawnie skonfigurowane i posiadające najbardziej aktualne oprogramowanie:

- instaluj aktualizacje bezpieczeństwa, natychmiast gdy tylko będą dostępne, aby w ten sposób „załatać" błędy, które przestępcy mogą wykorzystać;
- włącz automatyczne aktualizacje systemów operacyjnych, aplikacji i oprogramowania sprzętowego (tzw. firmware), jeśli możesz;
- zawsze korzystaj z najnowszych wersji systemów operacyjnych i aplikacji, aby korzystać z najnowszych funkcji bezpieczeństwa;
- konfiguruj zapory sieciowe, domyślnie blokując połączenia przychodzące.

Wskazówka 4: Ogranicz wpływ infekcji i umożliw szybką reakcję

Poniższe kroki zapewnią, że osoby reagujące na incydenty będą mogły pomóc Twojej organizacji szybko dojść do normlanego funkcjonowania po ataku:

- Pomóż zapobiegać w rozprzestrzenianiu się szkodliwego oprogramowania w całej organizacji. Zapobiegnie to swobodnemu przemieszczaniu się atakujących po urządzeniach w sieci w Twojej organizacji. Zapobiegnie to pozyskaniu poświadczeń uwierzytelniania lub wykorzystania narzędzi wbudowanych.
- Do uwierzytelniania użytkowników stosuj uwierzytelnianie wieloskładnikowe (MFA), a w szczególności uwierzytelnianie dwuskładnikowe (2FA). Nawet jeśli szkodliwe oprogramowanie wykradnie poświadczenia, nie można będzie ich ponownie użyć.
- Upewnij się, że nieaktualizowane systemy operacyjne i aplikacje są odpowiednio oddzielone od reszty sieci.
- Regularnie sprawdzaj i usuwaj nieużywane już uprawnienia użytkownika, aby ograniczyć możliwość rozprzestrzeniania się szkodliwego oprogramowania. Szkodliwe oprogramowanie może rozprzestrzeniać się tylko do miejsc w sieci, do których mają dostęp konta zainfekowanych użytkowników.

- Administratorzy systemu powinni unikać korzystania ze swoich kont administratora do obsługi poczty e-mail i przeglądania stron internetowych, aby uniknąć uruchamiania szkodliwego oprogramowania z wysokimi uprawnieniami systemowymi.
- Zaprojektuj swoją sieć tak, aby interfejsy zarządzania były jak najmniej narażone na ataki.
- W ramach dobrego zarządzania zasobami prowadź rejestr stosowanych wersji oprogramowania zainstalowanych na urządzeniach, który będzie natychmiast dostępny w przypadku potrzeby szybkiej aktualizacji ich zabezpieczeń.
- Aktualizuj nadzorowaną i zarządzaną infrastrukturę, tak, jak aktualizujesz swoje urządzenia i nadaj priorytet urządzeniom, które wykonują funkcje związane z bezpieczeństwem w sieci (takie jak firewalle) i inne urządzenia łączące różne sieci.
- Opracuj procedurę reagowania na incydenty, stosuj ją i aktualizuj z każdą zmianą w organizacji.

Materiały

Opracowano na podstawie materiałów informacyjnych NCSC - National Cyber Security Centre, Narodowego Centrum Cyberbezpieczeństwa Zjednoczonego Królestwa. Odnośnik do strony zewnętrznej.