Bezpieczeństwo

Mobilne bezpieczeństwo w środowisku biznesowym: rozwój i zabezpieczenie BYOD

Paweł Wałuszko 22.07.2019

W ostatnich latach trend przynoszenia własnych urządzeń do pracy, czyli BYOD (z ang. „Bring Your Own Device"), stał się zjawiskiem na tyle powszechnym w naszych sieciach, że nikogo nie dziwi używanie prywatnego smartfonu do sprawdzania służbowego maila, aktualizowania stron firmowych spoza biura lub łączenia się z systemami CRM przez specjalistów z działu sprzedaży, którzy pracują „w terenie".

Z dużą pewnością można stwierdzić, iż jest to efekt naturalnego procesu „bottom-up". Chcemy pracować szybciej, łatwiej i według natychmiastowych potrzeb. Gdy laptop przestanie działać, naturalnie sięgamy po smartfon, niezależnie od tego, czy jest służbowy czy prywatny. Hasła przecież znamy, a współpracownicy z biura rozumieją, że sumiennie wykonujemy swoją pracę, nawet gdy używamy nieautoryzowanych urządzeń.

Minęły też czasy, gdy menedżerowie ds. IT mogli definitywnie zadecydować o infrastrukturze mobilnej, która wraz ze smartfonami była wdrażana na każdym szczeblu przedsiębiorstwa. Tak było za czasów gdy w korporacjach królował BlackBerry, a urządzenia kanadyjskiej firmy RIM w każdej firmie były odgórnie zarządzane przez oprogramowanie „BlackBerry Enterprise Server".

W pewnym sensie, wszystkiemu zawinił iPhone. Odkąd Steve Jobs wszedł na scenę trzymając nowy gadżet, smartfony fundamentalnie się zmieniły – nie tylko pod względem powierzchownego wyglądu, ale także pod względem technologicznym. W przeciwieństwie do systemów opartych na technologii BlackBerry lub Symbian, iOS był innowacyjny w swojej prostocie. Przeglądarka, poczta, narzędzia biurowe – wszystko działało praktycznie od ręki, a użytkownicy zachwyceni ergonomicznym interfejsem iOS przynieśli urządzenia Apple do biur, żądając, aby ich ulubione smartfony również obsługiwały procesy biznesowe. Z pewną śmiałością można stwierdzić, że rewolucja BYOD zaczęła się właśnie od sukcesu iPhona, w 2007 roku.

W tamtym czasie iOS był pierwszym powszechnie znanym systemem, oferującym rozszerzony zakres usług i aplikacji, które z zasady były dostępne tylko na urządzeniach typu komputer stacjonarny lub laptop. Android natomiast dopiero się rozwijał i zadebiutował na amerykańskim rynku w 2008 r.

Dziś rynek smartfonów wygląda diametralnie inaczej. Smartfony to praktycznie pełnowymiarowe urządzenia, które de facto zastępują nam komputer. Niektóre modele nawet mogą być podłączone do monitorów i klawiatur, aby w pełni pracować jako komputer stacjonarny w naszym biurze. Natomiast w dziedzinie systemów operacyjnych, w ostatnich latach Android zdetronizował system od Apple, dziś obsługując ok. 86% smartfonów na świecie[1]. Jak można zauważyć, używanie miniaturowych, mobilnych komputerów do celów biznesowych ewidentnie nam się spodobało ponad dekadę temu i do dziś kontynuujemy rozwój właśnie w tą stronę.

Problematyczne systemy mobilne

Niestety, nie wszystko, co jest wygodne dla użytkownika, jest dobre dla właścicieli biznesów. Pracownicy korzystający w pracy z własnych telefonów z różnymi wariantami systemu Android mogą generować sporo problemów.

Po pierwsze, urządzenia zewnętrzne z natury funkcjonują poza pełną kontrolą administratora sieci w firmie. Nieostrożny użytkownik może więc z łatwością przynieść różnego typu złośliwe oprogramowanie do sieci firmowej, nawet nie zdając sobie z tego sprawy.

Po drugie, nawet przy fabrycznie nowych telefonach, istnieje problem tak zwanego „bloatware'u". Bloatware to dodatkowe, czasami niepożądane oprogramowanie dostarczane przez producenta na komputerach, smartfonach i tabletach. Najczęściej występuje w postaci nakładki na interfejs, kilkudniowej licencji na płatne oprogramowanie (tak zwany „trial") lub aplikacji zachęcającej do zakupienia dodatkowej obsługi.

Problem bloatware'u na komputerach Windows z zasady był rozwiązywany poprzez zwykłą de-instalację niepożądanego oprogramowania. Niestety, na systemach mobilnych, szczególnie na Androidzie, usuwanie takiego oprogramowania jest dość często niewykonywalne bez rootwania urządzenia, co znów automatycznie powoduje utratę gwarancji producenta.

Tymczasem bloatware stwarza poważne problemy dla bezpieczeństwa urządzeń mobilnych. Według najnowszych badań przeprowadzonych przez naukowców i badaczy z Universidad Carlos III de Madrid, Stony Brook University, IMDEA Networks Institute i ICSI, oprogramowanie typu bloatware na systemach mobilnych rutynowo obchodzi zabezpieczenia systemu operacyjnego, na którym się znajduje. Ponadto, znaczna część oprogramowania bloatware zbiera ogromne ilości danych o użytkownikach telefonów, mając dostęp do praktycznie wszelkich zasobów na urządzeniu.[2]

Administrator vs natura ludzka

Naturalnie, administratorzy ds. IT nie są obojętni wobec takich zagrożeń. Zważywszy na rosnący trend BYOD, niektóre firmy zaakceptowały tą tendencję i wdrożyły oprogramowanie mające na celu zarządzanie bezpieczeństwem platform mobilnych.

Inne przedsiębiorstwa podeszły do rozwiązania tego problemu połowicznie – np. poprzez stworzenie oddzielnego VLANu dla prywatnych urządzeń pracowników – i tym sposobem ograniczyły lub mocno zawęziły dostęp do usług sieci firmowej. Jeszcze inne wprowadziły całkowity zakaz korzystania z własnych telefonów w pracy, zezwalając wyłącznie na użytkowanie smartfonów i tabletów zakupionych i zabezpieczonych przez firmę.

Niestety, wprowadzenie zakazu BYOD nie przynosi wielu realnych rezultatów w dziedzinie bezpieczeństwa. Według badań przeprowadzonych w 2016r. dla firmy Samsung, około 55% pracowników niższego i średniego szczebla regularnie używa służbowych telefonów do celów prywatnych (mimo odgórnych obostrzeń).[3] Ci użytkownicy przechowują prywatne pliki w pamięci urządzenia, instalują dodatkowe aplikacje, lub co gorsze – korzystają z sideloadingu – czyli wgrywania własnych aplikacji w formacie pliku .apk, gdy aplikacja nie jest dostępna na zabezpieczonych platformach Google Play.

Jeżeli ktoś uważa, że wyżej wymieniony problem dotyczy tylko i wyłącznie pracowników niższego i średniego szczebla, bardzo się myli. Według tego samego badania, około jedna trzecia dyrektorów i osób zarządzających popełnia ten sam błąd, tylko że w ich wypadku, dostęp do danych poufnych dość często jest bardziej obszerny, niż tych pierwszych.

Tymczasem eksperci IDG biją na alarm. Według badania przeprowadzonego w 2019r. w oparciu o 100 liderów zarządzania usługami IT z różnych branż, takich jak sektor zaawansowanych technologii, usług finansowych i produkcji, 74% respondentów zgłosiło, że ich organizacje doświadczyły naruszenia ochrony danych w wyniku problemów związanych z bezpieczeństwem urządzeń mobilnych.

Jak rozwiązać problem z infrastrukturą mobilną?

Problemy wynikające z ludzkiej natury nie zawsze można rozwiązać za pomocą technologii. Ilustruje nam to sam fakt, że niezależnie od naszej polityki względem BYOD, użytkownicy mają tendencję do korzystania z rozwiązań, które po prostu są wygodne. Pracownicy bardzo często używają prywatnego urządzenia do sprawdzania służbowej poczty, na służbowych telefonach przechowują prywatne pliki, a nawet dzielą się hasłami. Czym jest to spowodowane? Najczęściej winny jest brak wiedzy w zakresie potencjalnych zagrożeń, które takie zachowania przynoszą.

Warto jest zauważyć, że niezależnie od naszego zabezpieczenia technologicznego w postaci systemów zarządzania urządzeniami mobilnymi, oprogramowania antywirusowowego, zapór i skanerów malware, najsłabszym punktem bezpieczeństwa sieci z zasady jest człowiek.[4] W związku z tym, podobnie jak w przypadku ataków socjotechnicznych, nie istnieje technologiczne rozwiązanie,

które zapewni nam stuprocentowe zabezpieczenie przed błędami ludzkimi. **Natomiast odpowiednie szkolenie w zakresie bezpieczeństwa jest jednym z najskuteczniejszych rozwiązań w zakresie podnoszenia świadomości bezpieczeństwa.** [5]

Poza inwestycją w wiedzę swoich współpracowników, kolejnym dobrym krokiem w dziedzinie bezpieczeństwa systemów mobilnych jest **audyt naszych urządzeń**.

W ramach audytu upewnijmy się, że wszystkie aplikacje użytkowników pochodzą od zweryfikowanych źródeł, takich jak Google Play. Owo repozytorium aplikacji mobilnych regularnie sprawdza oprogramowanie pod względem kompatybilności z różnymi wersjami systemu operacyjnego Android oraz pod względem bezpieczeństwa. Instalując aplikacje z Google Play już mamy dość dużą pewność, że malware nam się nie wkradnie.

Po drugie, usuńmy bloatware. Choć nie każdy smartfon ma możliwość usunięcia aplikacji wgranych przez producenta, część producentów zezwala na deaktywację niepożądanych aplikacji. Przy dezaktywacji aplikacja zostaje w pamięci naszego urządzenia, ale przestaje korzystać z danych, które znajdują się w naszym telefonie.

Po trzecie, sprawdźmy preferencje dostępu każdej aplikacji oraz ograniczajmy dostęp do przesyłania danych w tle. Jeżeli nie możemy usunąć niektórych aplikacji, system Android pozwala nam zarządzać dostępem do danych, takich jak lokalizacja, poczta, treści wiadomości tekstowych i wiele innych. Ustawienie indywidualnych preferencji dostępu według zdrowego rozsądku już powinno ograniczyć dostęp i przesyłanie danych przez aplikacje, które z zasady nie muszą korzystać z takiego dostępu. Ponadto, zawsze możemy ograniczyć przesyłanie danych w tle, co oznacza, że jeżeli nie używamy danej aplikacji, nie będzie miała ona możliwości wysyłania danych poza naszą kontrolą.

Na koniec, warto jest zainwestować w automatyzację wykrywania anomalii w sieci.

Ataki DoS (Denial of Service), niepożądane zachowania użytkowników i ich smartfonów da się wykryć za pomocą oprogramowania do monitorowania sieci. Przy odpowiedniej konfiguracji oprogramowania typu NMS (Network Monitoring Software) oraz powiązanych skryptów korygujących, możemy stworzyć platformę, która automatycznie zacznie proces zabezpieczania urządzenia lub konta użytkownika, gdy wykaże ono podejrzane zachowania. Ponadto, system monitorujący może nam wskazać konta użytkowników najczęściej naruszających wewnętrzną politykę bezpieczeństwa. Są to osoby, które powinny przejść dodatkowe szkolenie z dziedziny podstaw bezpieczeństwa i polityki ochrony danych firmy.

Podsumowanie

Niezależnie od tego, jakie mamy podejście do systemów mobilnych i BYOD w naszych sieciach firmowych, czynnik ludzki będzie nam towarzyszył. Niestety, nie istnieje rozwiązanie technologiczne, które może nam zagwarantować niepodważalne bezpieczeństwo. Warto jest zatem (oprócz rutynowego przeprowadzania audytów urządzeń mobilnych), zainwestować w rozwój pracowników w zakresie bezpieczeństwa,.

Wykorzystajmy też potencjał naszych działów IT i ich możliwości technologiczne we wczesnym wykrywaniu anomalii i niepożądanych zachowań. Przy niewielkim lub zerowym nakładzie finansowym, możemy wyposażyć nasz dział IT w system, który proaktywnie zadba o nasze bezpieczeństwo oraz wykryje, którzy pracownicy wymagają dodatkowego szkolenia z dziedziny bezpieczeństwa. Pamiętajmy, że bez odpowiedniego szkolenia pracowników, technologiczne rozwiązania w dziedzinie bezpieczeństwa przyniosą umiarkowane rezultaty.

1. IDC Corporate USA: *Smartphone Market Share.*
https://www.idc.com/promo/smartphone-market-share/os

2. Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, Narseo Vallina-Rodriguez. *An Analysis of Pre-Installed Android Software.* IMDEA Networks Institute, Universidad Carlos III de Madrid, Stony Brook University, ICSI.
/https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf

3. TNS – Samsung Electronics Polska. *„Samsung Mobile Workplace – Telefon komórkowy w środowisku biznesowym*". 14.07.2016 – 27.07.2016.

4. IBM: *IBM Security Services 2014 Cyber Security Intelligence Index, „Analysis of cyber attack and incident data from IBM's worldwide security operations."* PDF.; CIO/IDG: *Humans are (still) the weakest cybersecurity link.*
https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecurity-link.html

Kaspersky: *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within.* https://www.kaspersky.com/blog/the-human-factor-in-it-security/

5. CSO/IDG: *Employee training remains the best first line of defense against cybersecurity breaches.* https://www.csoonline.com/article/3237949/employee-training-remains-the-best-first-line-of-defense-against-cybersecurity-breaches.htmlPCI Security Standards: *Best Practices for Implementing a Security Awareness Program.* https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

22.07.2019

Paweł Wałuszko

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

Pizza Day – socjotechnika czai się wszędzie

Szukaj

Wprowadź frazę i wciśnij enter.

Najnowsze wpisy

Mobilne bezpieczeństwo w środowisku biznesowym: rozwój i zabezpieczenie BYOD

Pizza Day – socjotechnika czai się wszędzie

Program Zarządzania Podatnościami VMP (Vulnerability Management Program) – zarządzanie przedsiębiorstwem w procesie bezpieczeństwa IT

OSINT, czyli biały wywiad – metoda pozyskiwania informacji z cyberprzestrzeni w oparciu o dane jawnoźródłowe

WordPress: najbardziej zhakowany CMS na świecie. Jak nie stać się częścią statystyk?

Archiwum

Lipiec 2019
Czerwiec 2019
Kwiecień 2019
Marzec 2019
Styczeń 2019
Grudzień 2018
Listopad 2018
Sierpień 2018
Lipiec 2018
Maj 2018

Kwiecień 2018

Luty 2018

Styczeń 2018

TestArmy CyberForces

Usługi

- Testy Bezpieczeństwa
- Audyt Bezpieczeństwa
- Red Teaming
- Testy Penetracyjne
- Bezpieczne Wytwarzanie Oprogramowania
- Program Cyberbezpieczeństwa
- Testy Socjotechniczne
- Cyfrowe Bezpieczeństwo osób decyzyjnych

Branże

- Fintech
- E-commerce
- Software Houses

Firma

- Kontakt
- Blog
- Kariera

Wiedza

- Ebooki i Raporty

Skontaktuj się

info@cyberforces.com

+ 48 505 372 810

TestArmy CyberForces Sp. z.o.o.
ul. Petuniowa 9/5
53-238 Wrocław
Polska