Porady

Jak prezesi padają ofiarami hakerów. Przykład Jeffa Bezosa

Paweł Wałuszko 24.02.2020

W 2013 roku aktywista Edward Snowden oznajmił światu to, co wielu informatyków przewidywało już od dawna: fakt, że jesteśmy śledzeni przez nasze urządzenia. Choć jeszcze rok wcześniej zaklejanie kamerki internetowej w laptopie powszechnie uważano za przejaw paranoi, od tego czasu różnego rodzaje blokady kamer stały się hitowym gadżetem na każdej konferencji branży IT.

Obecnie minęło już wiele czasu, odkąd pogodziliśmy się z prawdą: nasze komputery nas śledzą. Instalujemy zapory, skanujemy systemy przed malware'em, dodajemy wtyczki blokujące ciasteczka w przeglądarce. Doskonale wiemy, że każdy nasz ruch jest śledzony przez „Wielkiego Brata" – Google. Dzięki wyciekom dostrzeżonym przez Snowdena, w pewnym sensie nauczyliśmy się dbać o naszą prywatność podczas korzystania z komputera, choćby poprzez powierzchowne zaklejanie kamery, które stało się bardzo powszechne.

Niestety wciąż często zapominamy o systemach mobilnych. Smartfony towarzyszą nam na co dzień. Nieraz używamy ich jako zamiennika komputera stacjonarnego i niejednokrotnie pozwalamy, aby łączyły nasze życie prywatne z biznesowym – choćby poprzez posiadanie kilku komunikatorów naraz. Są też one dodatkowo wyposażone w większą niż komputery stacjonarne, ilość kamer o wysokiej rozdzielczości, dobrej jakości mikrofony 360 stopni, chipy GPS i wiele innych funkcjonalności, które czynią z nich idealny przyrząd do monitorowania człowieka i jego środowiska.

Choć jesteśmy świadomi tego potencjału, zaklejanie kamerek w smartfonie jest praktycznie niespotykane. Instalujemy aplikacje, akceptując domyślne ustawienia dostępu do zasobów urządzenia – często nawet nie zwracamy na uwagi na ten komunikat. Gdy czegoś nie znajdziemy w Google Play, korzystamy z sideloadingu. Otwieramy pliki bez zastanowienia się, co zawierają i synchronizujemy mailowe skrzynki prywatne i biznesowe na jednym urządzeniu. Cieszymy się z ergonomii i wygody korzystania ze smartfonów ułatwiając sobie życie – i teoretycznie nie ma w tym nic złego, ale być może jednocześnie traktujemy systemy mobilne zbyt pobłażliwie?

Prezesi również padają ofiarami ataków

Najlepszym przykładem, dlaczego nie powinniśmy lekceważyć pułapek bezpieczeństwa systemów mobilnych, jest przypadek samego prezesa Amazonu – Jeffa Bezosa.

W 2018 roku, podczas rozmowy przez popularny komunikator WhatsApp, Bezos otrzymał wiadomość od osoby podającej się za księcia koronnego Arabii Saudyjskiej, Mohammeda bin Salmana. Jak donoszą media, wiadomość zawierała klip wideo, w którym znajdowały się dodatkowe linie kodu, pozwalające na import malware'u na urządzenie. Po aktywacji na telefonie Bezosa, malware dostał się do niemal wszystkich zasobów, dając hakerom nieograniczony dostęp do danych z telefonu. W mgnieniu oka okazało się, że prezes jednej z największych firm informatycznych jest tak samo podatny na ataki hackerskie jak przeciętny Kowalski.

Chwila nieuwagi może wiele kosztować

Od momentu zhackowania media spekulują, czy istnieje korelacja pomiędzy wyciekiem danych z iPhone'a Jeffa a rychłym rozwodem z MacKenzie Bezos. Nie jest jasne też, czy na wycieku nie ucierpiał sam Amazon. Faktem jest, że malware uzyskał dostęp do wszelkiej komunikacji na urządzeniu, w tym kont mailowych – można więc przypuszczać, że ujawnione zostały również kontakty biznesowe Bezosa.

Wycieki danych kosztują wiele – nie tylko miliarderów. Według statystyk Nortona, tylko w pierwszym półroczu 2019 roku, ujawnionych zostało ponad 4 miliardy poufnych dokumentów, co stanowi wzrost o 54% względem analogicznego okresu czasu w poprzednim roku. Co więcej, do końca września, liczba ta wzrosła do niemal 9 miliardów, co stanowi wzrost o kolejne 33%. Łącznie, według prognoz Juniper Research, cyberprzestępczość kosztowała przedsiębiorstwa ponad 3 biliony dolarów w 2019 r., a koszt wycieku jednego poufnego dokumentu – niezależnie od branży – IBM oszacował na 150 dolarów amerykańskich.

Biorąc pod uwagę, jak wiele danych może zostać ujawnionych przez uzyskanie dostępu do tylko jednego korporacyjnego konta mailowego, łatwo jest wyobrazić sobie realne koszty takiego wycieku w firmie. Smartfony, natomiast, dość często posiadają wiele takich kont, nie mówiąc już o dostępie do wewnętrznych komunikatorów i platform obsługujących procesy biznesowe.

Kogo atakują hakerzy

Z udanego ataku na smartfona prezesa Amazonu można wydedukować, że praktycznie każdy telefon może zostać zhackowany – wystarczy, że haker będzie odpowiednio zmotywowany. Pytaniem zasadniczym staje się więc nie to, czy da się kogoś zhackować, tylko kto wart jest takiej inwestycji.

Najprostsza odpowiedź brzmi: „osoby zarządzające".

Według najnowszego raportu Verizon 2019 „Data Breach Investigations Report", kierownictwo wyższego szczebla, czyli osoby mające dostęp do najbardziej poufnych informacji w firmie, są obecnie głównym obiektem ataków z wykorzystaniem inżynierii społecznej. Jak dowodzi Verizon, **„menedżerowie wyższego szczebla są 12 razy bardziej narażeni na ataki socjotechniczne i 9 razy bardziej podatni na wycieki danych niż w poprzednim roku"**.

Dlaczego tak się dzieje?

Głównym powodem ataków na menedżerów są korzyści finansowe płynące z dostępu do danych osób decyzyjnych. W porównaniu do przeciętnych pracowników, menedżerowie posiadają większy zakres dostępu do danych poufnych oraz możliwość poruszania się po całym budynku, podpisują umowy z kontrahentami i niejednokrotnie posiadają przywileje administratora na platformach biznesowych. Przechwytywanie własności intelektualnej jest lukratywnym biznesem, a sposobów monetyzacji tejże jest wiele.

Winny jest też sposób, w jaki używamy naszych smartfonów. Przeciętny smartfon w środowisku korporacyjnym ma dostęp do kont mailowych, systemów CRM i dokumentów poufnych. Co więcej, często jest używany jako urządzenie uwierzytelniające tożsamość użytkownika. To właśnie smartfon, gdy stracimy dostęp do hasła, jest domyślnym sposobem weryfikacji, na przykład poprzez odbiór wiadomości SMS. Niestety ta funkcjonalność czyni z nich idealne narzędzie do przechwytywania haseł i obchodzenia zabezpieczenia uwierzytelnienia dwuetapowego.

Mała powierzchnia ekranów smartfonów wymusza też pewne decyzje dotyczące ergonomii UI (interfejsu aplikacji). Najczęściej używane elementy interfejsu zajmują zwykle pierwsze miejsce, a zaawansowane funkcje, dość często dotyczące bezpieczeństwa danych, są usuwane lub chowane wewnątrz menu (z którego niekoniecznie korzystamy). To wszystko wpływa negatywnie na kwestie bezpieczeństwa.

Co zrobić, aby nie stać się częścią statystyk?

Rozmiaru ekranów naszych smartfonów raczej nie zmienimy – straciłyby wtedy one na ergonomiczności. Usuwanie z telefonów kont mailowych i komunikatorów też nie ma sensu – mijałoby się to z celem posiadania tych urządzeń.

Nie oznacza to jednak, że powinniśmy poddać się bez walki i korzystać ze smartfonów tylko i wyłącznie w oparciu o nadzieję, że nic przykrego nam się nie stanie. Możemy – i powinniśmy! – podjąć pewne działania, które pozwolą nam bezpieczniej korzystać z tych urządzeń bez drastycznego ograniczania ich funkcjonalności.

Oddzielmy życie prywatne od służbowego

Zakładając, że posiadamy dwie karty SIM – jedną prywatną i jedną służbową – najlepszym rozwiązaniem jest używanie ich w dwóch różnych urządzeniach. Po pierwsze, używając urządzenia prywatnego do kontaktu wyłącznie z bliskimi, mamy pełną swobodę dotyczącą aplikacji i zabezpieczeń, z których korzystamy. Nie musimy starać się o aprobatę administratora przy każdej zmianie i nie obowiązuje nas polityka bezpieczeństwa danych firmy, która może być wymuszona przez platformy MDM (Mobile Device Management). Po drugie, narażenie jednego urządzenia, nawet w całości (jak to się przydarzyło Jeffowi Bezosowi) nie pociągnie za sobą utraty danych z kont służbowych.

O ile to możliwe, stosujmy zasadę „physical security is the best security", czyli „bezpieczeństwo fizyczne jest najlepszym zabezpieczeniem". Znając hasła do systemów biznesowych, nigdy nie używajmy ich na urządzeniach prywatnych – nawet gdy wymusza to nagła sytuacja.

Twórzmy bariery w zakresie funkcjonalności urządzenia

Jeżeli jednak bardzo zależy nam, aby korzystać z jednego urządzenia do służbowego i prywatnego użytku, wykorzystujmy w ten sposób urządzenie pracodawcy, ale zainwestujmy w narzędzia do profesjonalnego zarządzania jego bezpieczeństwem, w postaci platform MDM.

W przeciwieństwie do urządzeń prywatnych smartfony biznesowe przechodzą testy bezpieczeństwa i proces „security hardening", czyli zabezpieczanie luk w oprogramowaniu i usuwanie aplikacji, które mogą nadużywać dostęp do zasobów smartfona. Ponadto, platformy MDM umożliwiają konteneryzację aplikacji, co oznacza, że aplikacje służbowe (teoretycznie) nie mają dostępu do informacji i danych prywatnych aplikacji użytkownika.

Używając smartfonów profesjonalnie zarządzanych przez dział IT, mamy większą pewność, że są one lepiej zabezpieczone, a narzucona polityka instalowania dodatkowych aplikacji chroni nas przed malware'em. Najgorszą praktyką natomiast jest korzystanie z urządzeń prywatnych w celu logowania się do systemów biznesowych – tutaj pracodawca narażony jest na wszelkiego typu ataki, które mogą pochodzić z aplikacji, funkcjonujących poza możliwością weryfikacji bezpieczeństwa.

Pamiętajmy też o weryfikacji dwuetapowej. Jeżeli używamy jednego urządzenia do np. odbierania maila i wiadomości tekstowych, nie powinno ono być również naszym narzędziem do wspomnianej weryfikacji. Popularną metodą jest tworzenie np. klucza USB lub weryfikacji głosowej za pomocą innego numeru telefonu. Jeżeli to samo urządzenie ma dostęp do maila i jest domyślnym urządzeniem weryfikującym tożsamość, cała weryfikacja dwuetapowa zupełnie traci swoją wartość obronną.

Inwestujmy w wiedzę i stosujmy dobre praktyki korzystania ze smartfonów

Ataki socjotechniczne są atakami psychologicznymi, które wykorzystują naturę ludzką i pewne słabości w procesie podejmowania decyzji, które nam towarzyszą. Osoby na stanowiskach kierowniczych w pewnym sensie skazane są na stres, brak czasu i pracę w trybie wielozadaniowym. Wszystko to przyczynia się do podejmowania pochopnych decyzji, np. w przypadku Jeffa Bezosa braku weryfikacji czy wiadomość faktycznie pochodziła od tego nadawcy i otwarciu nieznanego załącznika.

Niestety nie ma jednej złotej rady, jak zapobiegać atakom socjotechnicznym. Również żadne rozwiązanie technologiczne nie jest w stanie zagwarantować nam stuprocentowego bezpieczeństwa danych, w szczególności tych na systemach mobilnych. Regularny audyt zainstalowanych aplikacji, świadomość standardów bezpieczeństwa i wiedza dotycząca tego, jakie formy ataków są aktualnie wykorzystywane do hakowania smartfonów, to najlepsza ochrona przed atakami technologicznymi i socjotechnicznymi.

Źródła:

Norton. *Emerging Threats: 2019 data breaches: 4 billion records breached so far.*

RBS, *Q3 2019 Data Breach QuickView Report.*

Juniper Research. *The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024.*; IBM. Cost of a Data Breach Report, 2019.

Verizon. *2019 Data Breach Investigations Report.*

24.02.2020

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.

OPSEC, czyli sztuka ochrony danych według armii USA

Jak zwiększyć prywatność w sieci? Garść sprawdzonych porad

Szukaj

Wprowadź frazę i wciśnij enter.

Najnowsze wpisy

- Analiza zagrożeń. Jak się za to zabrać?
- Konferencje cybersecurity 2020. Aktualna lista
- Jak zwiększyć prywatność w sieci? Garść sprawdzonych porad
- Jak prezesi padają ofiarami hakerów. Przykład Jeffa Bezosa
- OPSEC, czyli sztuka ochrony danych według armii USA

Archiwum

- Marzec 2020
- Luty 2020
- Styczeń 2020
- Grudzień 2019
- Październik 2019
- Sierpień 2019
- Lipiec 2019
- Czerwiec 2019
- Kwiecień 2019
- Marzec 2019
- Styczeń 2019
- Grudzień 2018
- Listopad 2018
- Sierpień 2018
- Lipiec 2018
- Maj 2018