**Co nam grozi ze strony hakerów w 2016r?**

**Szybki wzrost liczby nowych, nieznanych typów złośliwego oprogramowania, podatność urządzeń mobilnych na ataki oraz luki w zabezpieczeniach najczęściej używanych systemów operacyjnych (Android, iOS i innych) – to trzy największe zagrożenia bezpieczeństwa w 2016 roku według ekspertów firmy Check Point.**

Specjaliści firmy Check Point wskazują, że już w tym roku 42% organizacji padło ofiarą skutecznych ataków wymierzonych w urządzenia mobilne a koszty likwidacji skutków tych incydentów przekroczyły 1 mln zł. Co więcej, 82% badanych firm spodziewa się wzrostu liczby takich incydentów. W bieżącym roku głośne stało się wykrycie kilku poważnych luk w zabezpieczeniach urządzeń mobilnych, m.in. [Certifigate](http://blog.checkpoint.com/2015/08/06/certifigate/) w smartfonach z systemem Android oraz XcodeGhost w iOS.

Hakerzy nieustannie odkrywają nowe sposoby atakowania sieci – czego dowodzą głośne w tym roku włamania do systemów Anthem, Experian, Carphone Warehouse, Ashley Madison i TalkTalk.

Oto lista dziesięciu tendencji i zagrożeń, na jakie, zdaniem firmy Check Point, narażone będą systemy komputerowe w 2016 roku:

l  **Złośliwe oprogramowanie typu „snajper” i „shotgun”**

Spodziewamy się, że najpoważniejsze włamania do systemów komputerowych w 2016 roku będą wynikiem specjalnie tworzonego oprogramowania, zdolnego przeniknąć do systemów konkretnych organizacji; przykładem takiego włamania może być atak na system amerykańskiego przedsiębiorstwa handlowego Target. Wprawdzie niespecyficzne ataki o szerokim zasięgu będą nadal zagrożeniem dla osób fizycznych i małych firm, lecz hakerzy poświęcą więcej uwagi atakom na wybrane duże organizacje.

l  **Więcej ataków na urządzenia mobilne**

Częstotliwość ataków na urządzenia mobilne będzie się nadal zwiększać, w miarę, jak urządzenia te będą coraz powszechniej używane w miejscu pracy. Hakerzy mogą w ten sposób zdobywać bezpośredni i potencjalnie przynoszący im duże korzyści finansowe dostęp do poufnych danych osób fizycznych i korporacji.

l  **Zapobieganie zagrożeniom**

W toczącej się wojnie między hakerami i specjalistami od bezpieczeństwa komputerowego napastnicy stosują coraz bardziej zaawansowane techniki, wyspecjalizowane wersje znanego już wcześniej złośliwego oprogramowania oraz eksploity „zero-day”, przeciwko którym tradycyjna technologia piaskownicy jest bezsilna.

l  **Ataki na kluczowe elementy infrastruktury**

W grudniu 2014 roku system informatyczny niemieckiej huty stali padł ofiarą ataku, w wyniku którego hakerzy przeniknęli do sieci zakładu produkcyjnego i spowodowali ogromne szkody. Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych poinformował także, że infekcja oprogramowaniem typu „koń trojański” spowodowała naruszenie bezpieczeństwa przemysłowych systemów sterowania w ponad tysiącu zakładów energetycznych w Europie i Ameryce Północnej. Ataki na obiekty użyteczności publicznej i ważne instalacje przemysłowe nie ustaną i będą wykorzystywać złośliwe oprogramowanie, którego celem są systemy SCADA używane do sterowania procesami.

l  **IoT i urządzenia wyposażone w inteligencję**

Technologia IoT (Internet przedmiotów) pozostaje na wczesnym etapie rozwoju i nie zanosi się na to, aby miała odegrać ważną rolę w 2016 roku. Niemniej jednak organizacje powinny już dziś myśleć o tym, jak zabezpieczyć swoje urządzenia wyposażone w inteligencję oraz przygotować się do upowszechnienia się technologii IoT. Użytkownicy powinni przede wszystkim zadać sobie dwa pytania: „Dokąd trafiają moje dane?” i „Co by się stało, gdyby ktoś uzyskał dostęp do tych danych?”

l  **Dobrze się nosi**

Urządzenia elektroniczne przeznaczone do noszenia („wearables”), takie jak smartwatch, powoli przenikają do firm i powodują nowe zagrożenia i problemy. Dane zapisane w tych urządzeniach narażone są na różnego rodzaju ataki, a ponadto „wearables” mogą zostać wykorzystane przez hakerów, aby za pomocą oprogramowania typu „koń trojański” przejąć zdalną kontrolę nad kamerą i mikrofonem. Dlatego organizacje, które zezwalają na używanie takich urządzeń powinny zadbać o to, aby były one należycie zabezpieczone (szyfrowanie pamięci i silne hasła).

l  **Pociągi, samoloty i samochody**

W 2015 roku miały miejsce pierwsze ataki na systemy komputerowe instalowane w samochodach, prowadzące do przejęcia kontroli nad pojazdem. W lipcu firma Fiat Chrysler wycofała w Stanach Zjednoczonych 1,4 milionów samochodów Jeep Cherokee po wykryciu przez informatyków możliwości przejęcia kontroli nad pojazdem za pośrednictwem sieciowego systemu audiowizualnego. W związku z tym, że w nowoczesnych samochodach instaluje się coraz więcej gadżetów i systemów mających połączenie z siecią, konieczne jest stosowanie zabezpieczeń. To samo dotyczy skomplikowanych systemów obecnych w samolotach pasażerskich, pociągach i innych środkach transportu publicznego.

l  **Rzeczywiste bezpieczeństwo w wirtualnej rzeczywistości**

W ostatnich latach upowszechniła się w firmach technologia wirtualizacji w formie SDN, NFV i chmury obliczeniowej. Środowiska zwirtualizowane są skomplikowane i powodują, że pojawiają się nowe warstwy sieci. Dopiero teraz zaczynamy rozumieć, jak należy je zabezpieczać.

l  **Nowe środowiska, nowe zagrożenia**

W 2015 roku pojawiło się kilka nowych systemów operacyjnych, między innymi Windows 10 i iOS 9. W ostatnich latach większość ataków na korporacyjne systemy komputerowe wykorzystywała luki w systemie Windows 7, gdyż system Windows 8 był stosunkowo rzadko instalowany. Ponieważ system Windows 10 można pobrać za darmo, liczba instalacji szybko rośnie i zapewne przyciągnie uwagę cyberprzestępców, którzy spróbują wykorzystać słabości tych nowych systemów operacyjnych, częściej aktualizowanych i mniej znanych użytkownikom.

l  **Konsolidacja zabezpieczeń – nie komplikować!**

Aby zabezpieczyć systemy przed różnorodnymi zagrożeniami, eksperci będą częściej korzystać ze scentralizowanych rozwiązań do zarządzania bezpieczeństwem. Przy dużej liczbie różnych produktów służących do zapewnienia bezpieczeństwa korporacyjnej sieci konsolidacja umożliwia zarówno uproszczenie całego systemu, jak i zmniejszenie kosztów. Mnogość niezależnych od siebie produktów i rozwiązań sprawia, że zarządzanie nimi staje się praktycznie niemożliwe; mogą one nawet obniżać poziom bezpieczeństwa. Dlatego konsolidacja zabezpieczeń jest skutecznym sposobem uproszczenia procesu zarządzania, a także pozwala zapobiec pojawianiu się nowych zagrożeń w lukach między różnymi systemami.