(Nie)bezpieczne smartfony – czy technologia zabezpieczeń jest gotowa na nowe zagrożenia?

Smartfony i tablety są powszechnie wykorzystywane w biznesie. Ich mobilność i wygoda sprawiają, że użytkownicy nawet nie wyobrażają sobie powrotu do tradycyjnych telefonów. Jak w każdym przypadku rozwoju nowej technologii IT podąża za nim rozwój nowych zagrożeń, a krok za nim rozwój nowych środków ochrony przeciwdziałających tym zagrożeniom. W mediach pojawia się wiele informacji na ten temat. Ale czy w tym przypadku rzeczywiście mamy do czynienia z nowymi zagrożeniami, które wymagają zastosowania nowego podejścia do bezpieczeństwa?

dr inż. Mariusz Stawowski, CLICO

Aby odpowiedzieć na to pytanie, podejdziemy do tego jak do projektu zabezpieczeń nowego elementu systemu informatycznego, gdzie wykonamy analizę ryzyka i na jej podstawie ustalimy, jakie zabezpieczenia są potrzebne. Do celów tego artykułu wykonamy to na ogólnym poziomie.

Urządzenia i aplikacje mobilne w zastosowaniach biznesowych są niewątpliwie nowym elementem systemu informatycznego. W projektowaniu zabezpieczeń obowiązuje ogólna zasada, że zabezpieczenia są potrzebne, gdy ryzyko jest wysokie i nie może być zaakceptowane. Wielkość ryzyka jest uzależniona od trzech czynników – wielkości zagrożeń i podatności oraz wartości zasobów (wielkości strat), a redukowanie ryzyka odbywa się za pomocą zabezpieczeń. Czytelnicy, którzy nie zajmowali się wcześniej analizą ryzyka, mogą, patrząc na rysunek 1, łatwo zrozumieć te zależności.

Jaką wartość posiadają urządzenia mobilne?

Urządzenia mobilne i znajdujące się na nich aplikacje i dane są w wielu firmach istotnym zasobem systemu informatycznego. Wartość zasobu i wynikająca z niej wielkość strat dla firmy (w razie wystąpienia naruszenia bezpieczeństwa zasobu) można ogólnie oszacować w odniesieniu do tego, w jakim zakresie ten zasób jest wykorzystywany do wspomagania działalności biznesowej firmy. Zastosujemy tu podejście ilościowe i jakościowe. Ilościowo widzimy, że firmy kupują dla pracowników duże ilości smartfonów i tabletów, zwłaszcza dla kadry zarządzającej, która posiada dostęp do najcenniejszych informacji firmy.

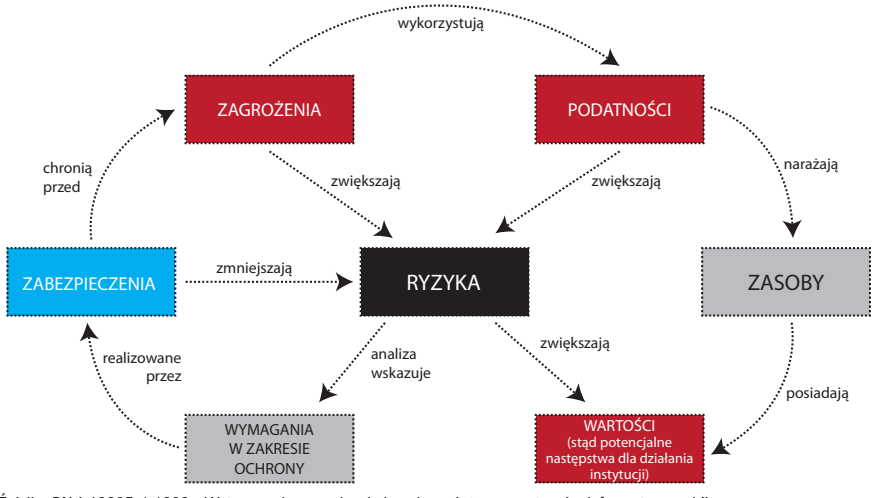
Smartfony i inne urządzenia mobilne w wielu firmach są używane do takich samych zadań, jak komputery, m.in.: poczta elektroniczna, CRM, ERP. Potencjalne konsekwencje naruszenia bezpieczeństwa dla urządzeń mobilnych są więc zbliżone do tych dla komputerów. Oznacza to, że dla wielu firm naruszenie bezpieczeństwa urządzeń mobilnych spowoduje poważne straty.

Zagrożenia i podatności urządzeń mobilnych

Zagrożenia urządzeń mobilnych są analogiczne jak komputerów. Do tej pory nie zostało zauważone nowe zagrożenie, istotne tylko dla urządzeń mobilnych. Tak samo jak dla komputerów do istotnych zagrożeń urządzeń mobilnych, które należy mieć na uwadze w zarządzeniu bezpieczeństwem, można zaliczyć:

- włamanie do urządzenia,
- infekcja urządzenia złośliwym kodem,
- kradzież urządzenia,
- awaria lub zablokowanie urządzenia,
- podsłuch sieciowy urządzenia,

RYS. 1. CZYNNIKI WPŁYWAJĄCE NA WIELKOŚĆ RYZYKA W SYSTEMACH INFORMATYCZNYCH



Źródło: PN-I-13335-1:1999, „Wytyczne do zarządzania bezpieczeństwem systemów informatycznych".

- włamanie do infrastruktury, z której korzystają urządzenia (WiFi, VPN itp.),
- ataki socjotechniczne.

Podatności urządzeń mobilnych są także podobne jak komputerów, ale ich wielkość jest już różna. Tabela 1 przedstawia istotne podatności urządzeń mobilnych oraz dostępne środki ochrony przeciwdziałające wykorzystaniu tych podatności. Dla porównania w tabeli zamieszczone zostały także dane dla komputerów.

Przyjrzyjmy się temu bliżej. W przypadku błędów systemu operacyjnego urządzenia mobile wypadają znacznie gorzej niż komputery. Większość komputerów na świecie korzysta z systemu operacyjnego Microsoft Windows. Działy IT w firmach wiedzą, w jaki sposób zapewnić komputerom z systemem Microsoft Windows regularną aktualizację, często dysponują narzędziami do centralnej instalacji i aktualizacji oprogramowania i co ważne mają świadomość konieczności wykonywania tych czynności. Urządzenia mobilne wykorzystują zaś wiele różnych platform i systemów operacyjnych, m.in. Apple iOS, Google Android OS, Nokia Symbian OS, Microsoft Windows Mobile/Phone, BlackBerry OS itd. Praktyka pokazuje, że urządzenia mobilne w wielu firmach nie są regularnie aktualizowane, co znacząco zwiększa ryzyko naruszenia ich bezpieczeństwa.

Znacznie lepiej w urządzeniach mobilnych wygląda sytuacja ze złośliwym kodem w aplikacjach. W przypadku komputerów ich użytkownicy mogą w praktyce uruchamiać dowolne aplikacje. Aplikacje dostępne są w bardzo wielu miejscach w internecie, gdzie nikt ich nie poddaje kontroli. W urządzeniach mobilnych wygląda to inaczej. Aplikacje można pobierać tylko z wyznaczonych repozytoriów oprogramowania (m.in. Apple App Store, Android Market, Windows MarketPlace). Znacznie trudniej niż dla komputerów można rozprowadzać aplikacje zawierające złośliwy kod, a po zidentyfikowaniu niebezpiecznych aplikacji znacznie łatwiej jest je usunąć z obiegu.

Należy przy tym jednak pamiętać, że kontrola aplikacji instalowanych na urządzeniach mobilnych jest skuteczna, gdy ich użytkownicy korzystają z nich w normalny sposób. Poprzez operacje eskalacji przywilejów (tzw. jailbreak w iOS, rooting w Android) użytkownicy mają możliwość podwyższenia swoich uprawnień na urządzeniu i korzystania z dowolnych aplikacji

TAB 1. ISTOTNE PODATNOŚCI I ŚRODKI IM PRZECIWDZIAŁANIA DOSTĘPNE W URZĄDZENIACH MOBILNYCH I KOMPUTERACH

Podatność (słabość zabezpieczeń)	Środki ochrony przeciwdziałające wykorzystaniu podatności	
	Komputery	Urządzenia mobilne
Błędy systemu operacyjnego i aplikacji	Regularna aktualizacja i hotfixy	
Złośliwy kod w aplikacjach	Antywirus	Kontrola App Store Uwaga: Jailbreak/rooting Antywirus (w zależności od dostępności)
Korzystanie z niebezpiecznych aplikacji	Zabezpieczenia sieciowe (np. NGFW, DLP) Centralny system monitorowania	Centralny system monitorowania
Mały rozmiar ułatwiający kradzież lub zgubienie urządzenia	Nie dotyczy	Szyfrowane danych Funkcje śledzenia Funkcje zdalnego usuwania danych
Wyłączenie zabezpieczeń przez użytkownika	Konto nieuprzywilejowane Centralny system monitorowania	Centralny system monitorowania
Słabo zabezpieczony dostęp WiFi	Bezpieczna infrastruktura WiFi Uwaga: Nie muszą korzystać z WiFi	Bezpieczna infrastruktura WiFi
Słabo zabezpieczony zdalny dostęp do sieci firmowej	Dedykowane rozwiązania VPN	Dedykowane rozwiązania VPN
Niska świadomość i ostrożność użytkowników	Znane zasady bezpieczeństwa	

Źródło: Opracowanie własne.

dostępnych w internecie. Dla firm stwarza to duże niebezpieczeństwo. Pracownicy powinni zostać uczuleni (np. w trakcie szkoleń *security awareness*), że takie praktyki są w firmie zabronione.

Przy analizowaniu podatności urządzeń mobilnych na szczególną uwagę zasługuje niska świadomość i ostrożność użytkowników tych urządzeń. W przypadku komputerów ludzie zwykle zdają sobie sprawę z niebezpieczeństw, na jakie są narażeni i starają się przestrzegać znane im zasady bezpieczeństwa (np. chronią komputer hasłem, nie klikają w linki umieszczone w wiadomościach e-mail, nie otwierają załączników email od nieznanych nadawców itp.). Z kolei w czasie korzystania ze smartfonów ostrożność użytkowników często jest wyłączona. Wynika to z wieloletniego przyzwyczajenia do beztroskiego korzystania z telefonów, gdzie w zakresie bezpieczeństwa nic szczególnego nie mogło się wydarzyć. Głównym zadaniem programu *security awareness* dla pracowników, którzy korzystają ze smartfonów powinno być dokładne wyjaśnienie im faktu, że smartfony to są komputery, a nie telefony. W smartfonach wykonywanie połączeń telefonicznych jest tylko jedną z wielu funkcji i pod względem bezpieczeństwa wymagają stosowania przez użytkowników zasad ochrony analogicznie jak komputery. Więcej informacji na ten temat można znaleźć m.in. w serwisie: www.bezpiecznypracownik.pl.

Jak bezpiecznie używać smartfonów i tabletów?

Korzystanie z urządzeń mobilnych w sposób bezpieczny dla biznesu firmy wymaga zastosowania środków technicznych i organizacyjnych adekwatnych do zagrożeń i podatności oraz potencjalnych strat, jakie firma poniesie w razie naruszenia bezpieczeństwa. Technologie zabezpieczeń dla urządzeń mobilnych oferowane są już przez znanych producentów (m.in. Check Point, Juniper Networks, Trend Micro itd.).

Do najistotniejszych czynności, które powinny zostać wykonane w firmach, gdzie smartfony i tablety wykorzystywane są do celów biznesowych, można zaliczyć:

1. Aktualizacja polityki bezpieczeństwa firmy o zapisy dotyczące urządzeń mobilnych.
2. Aktualizacja programu *security awareness* o zapisy dotyczące urządzeń mobilnych.
3. Wdrożenie centralnego systemu zarządzania urządzeń mobilnych (m.in. aktualizacja urządzeń, kontrola aplikacji i działań użytkowników, śledzenie i zdalne usuwanie danych).
4. Wdrożenie lokalnych zabezpieczeń na urządzeniach mobilnych (m.in. kontrola dostępu, VPN).

Oprócz tego firmy powinny zweryfikować stan bezpieczeństwa infrastruktury WiFi, z której korzystają urządzenia mobilne i w razie potrzeby ją udoskonalić. W praktyce zdarza się bowiem, że firmy, aby zapewnić smarfonom i tabletom dostęp do systemu informatycznego na szybko uruchamiają dostęp WiFi. Stwarza to dodatkowe zagrożenie nieupoważnionego dostępu do sieci firmowej. Podobnie sytuacja wygląda ze zdalnym dostępem do sieci firmowej (np. dla pracowników w podróży). Dostęp do sieci firmowej z zewnątrz powinien odbywać się przez odpowiednio zabezpieczony koncentrator VPN, tak samo jak dla zdalnego dostępu komputerów. Urządzenia mobilne nie są nowym złem. Zarządzając bezpieczeństwem urządzeń mobilnych, firmy mogą stosować metody i dobre praktyki, które są znane i od wielu lat z powodzeniem wykorzystywane w świecie komputerów.