Sophos udostępnia Mobile Security Toolkit - darmowy zestaw narzędzi przeznaczony do wzmocnienia ochrony urządzeń mobilnych

Sophos, firma specjalizująca się w technologiach ochrony informacji, opublikował wyniki badania przeprowadzonego przez TNS, niezależną grupę zajmującą się badaniami rynku. Badanie ujawnia nastawienie konsumentów do bezpieczeństwa urządzeń mobilnych i zapobiegania utracie danych. Mimo, że prawie jedna czwarta konsumentów (22%) zgubiła telefon komórkowy w przeszłości, a kolejne 12% straciło telefon w wyniku kradzieży, aż 67% nie ma utworzonego hasła na swoich komórkach w celu ochrony danych.

60% badanych uznało, że kradzież lub zgubienie urządzenia to największe zagrożenie dla bezpieczeństwa urządzeń mobilnych; jednak tylko 57% posiada zabezpieczenie hasłem nawet na laptopach, a 18% przyznaje się do używania tego samego hasła do wszystkiego.

Utrata urządzeń mobilnych, poza tym że dotyka bezpieczeństwa danych konsumentów, to również rosnący problem dla przedsiębiorstw, ponieważ coraz częściej używamy jednego urządzenia do pracy i zadań osobistych. W rzeczywistości, użytkownicy są jednym z najsłabszych ogniw w bezpieczeństwie organizacji, dlatego też menedżerowie IT kładą duży nacisk na edukację. Aby pomóc firmom w edukacji pracowników na temat zagrożeń związanych z technologią mobilną, Sophos udostępnił Mobile Security Toolkit - darmowy zestaw narzędzi zawierający najważniejsze porady dotyczące tworzenia bezpiecznych haseł, prezentację i poradnik wideo, whitepapers oraz przykładową politykę bezpieczeństwa dla urządzeń mobilnych.

"Coraz więcej ludzi wykorzystuje osobiste laptopy, smarfony i tablety do pracy zdalnej. Mimo że przyczynia się to do poprawy wydajności i innowacyjności w firmie, istotne jest, aby zadbać o kwestie bezpieczeństwa urządzeń mobilnych już teraz, zanim będzie za późno," powiedział James Lyne, kierownik ds. strategii technologii w Sophos. "Jeśli niezabezpieczony osobisty laptop pracownika wpadnie w niepowołane ręce, bardzo łatwo będzie można uzyskać dostęp nie tylko do informacji osobistych, ale także do jakichkolwiek dokumentów związanych z pracą zapisanych na dysku laptopa, a nawet wykorzystać komputer do połączenia się z siecią firmową."

Urządzenia mobilne zrewolucjonizowały sposób przechowywania, przesyłania i dostępu do informacji. Aby poradzić sobie ze zwiększonym ryzykiem utraty danych jakie niosą urządzenia przenośne, firmy muszą zagwarantować wsparcie dla wielu platform - szerokiej gamy systemów operacyjnych, za pośrednictwem których użytkownicy uzyskują dostęp do danych firmowych. Rozpowszechnienie smartfonów i tabletów, oraz różnice w systemach operacyjnych zainstalowanych na tych urządzeniach oznacza, że ryzyko potencjalnego ataku jest większe niż kiedykolwiek wcześniej. Firmy muszą więc wdrożyć politykę bezpieczeństwa, która zapewni ochronę sensytywnych danych, niezależnie od tego, jakie urządzenie ma do nich dostęp.

"Większość wycieków danych z urządzeń mobilnych ma miejsce głównie z powodu zaniedbania podstawowych zasad bezpieczeństwa; brak hasła lub słabe hasło, brak szyfrowania danych, padnięcie ofiarą phishingu lub innych ataków socjotechnicznych," kontynuował Lyne. "Jeśli urządzenia są wykorzystywane w celach służbowych, ważne jest, aby zespoły IT miały nad nimi podstawową kontrolę. Upewniając się, że urządzenia w przypadku zaginięcia mogą być w każdej chwili zdalnie wyczyszczone, firmy mogą zminimalizować ryzyko wycieku danych."

Sophos Mobile Security Toolkit można pobrać za darmo na stronie Sophos pod adresem:
http://www.sophos.com/en-us/security-news-trends/security-trends/mobile-security-toolkit

Sophos przygotował też krótki film na youtube, pokazujący dlaczego warto zabezpieczyć telefon:
http://www.youtube.com/watch?v=8nzuD5IX95k

Sophos