Nowe badanie prawie 1200 organizacji ujawniło głębokie zaniepokojenie kiepskim poziomem legislacji ochrony danych. Przeprowadzona przez Sophos ankieta pokazała, że niemal 50% chciałoby dalej idących regulacji prawnych, podczas gdy aż 87% uważa, że organizacje powinny być zmuszane do ujawniania informacji, gdy dojdzie do wycieku danych.

Badanie, którego celem była ocena poglądów respondentów na temat obecnego stanu prawnego ochrony danych, wykazało, że 41% martwi się dodatkową złożonością i idącymi za tym kosztami przestrzegania przepisów. Podczas gdy branża bezpieczeństwa rozwija narzędzia do walki z utratą danych - takie jak szyfrowanie, anty-malware i technologie ochrony przed utratą danych - dzisiejsze zespoły IT, z których duża część ma ograniczone budżety, chce prostego, ekonomicznego podejścia do ochrony danych.

"Ochrona danych jest poważnym problemem. Chcieliśmy lepiej zrozumieć dzisiejsze odczucia przedsiębiorstw," powiedziała Carole Theriault, konsultant ds. bezpieczeństwa w Sophos. "Wyniki badania pokazały, że informacje o wyciekach danych powinny być podawane do wiadomości publicznej, a to w mojej opinii oznacza, że jasne i zwięzłe wytyczne dla firm są wymagane. Ponieważ ustawodastwo różni się w zależności od regionu, nie ma możliwości ujednolicenia norm. Jednak zgodne, transgraniczne ramy prawne dotyczące ochrony danych uprościłyby kwestię zgodności oraz pomogły nam w komunikacji i szkoleniu firm na całym świecie."

Sophos przygotował dziesięć wskazówek, które pomogą firmom lepiej chronić swoje cenne dane:

1. Szyfruj wszelkie poufne informacje. Trzymaj poufne informacje z dala od nieupoważnionych.

2. Używaj trudnych do odgadnięcia haseł. Wykorzystywanie mocnych haseł jest kluczem do zatrzymania hakerów przed włamaniem do twoich systemów.

3. Dbaj o aktualizowanie oprogramowania bezpieczeństwa. Nowy malware jest wydawany przez cały czas i rozprzestrzenia się w alarmującym tempie. Aktualizowanie oprogramowania jest decydujące w walce z najnowszymi zagrożeniami i lukami w oprogramowaniu.

4. Uważaj na USB! Nieuprawnione użycie urządzeń pamięci masowej USB może doprowadzić do utraty firmowych danych. Kontroluj dostęp za pomocą odpowiedniego oprogramowania.

5. Wiedza to potęga. Dowiedz się, jakie wymogi prawne obowiązują w twoim regionie i sprawdź swoje polityki bezpieczeństwa, by zapewnić zgodność.

6. Przygotuj się do katastrofy. Stwórz plan działania, który zainicjujesz w przypadku naruszenia bezpieczeństwa danych. Szybka reakcja może stanowić ogromną różnicę jeśli wziąć pod uwagę konsekwencje prawne i reputację firmy.

7. Edukacja jest kluczem do sukcesu. Znajdź dobry sposób na wyjaśnienie pracownikom, jak dużą wartość mają dane - omów technologie, polityki i najlepsze praktyki bezpieczeństwa.

8. Zachęcaj - nie karaj - pracowników, którzy zgłosili potencjalną utratę lub naruszenie danych. Informacje te mogą pomóc złagodzić przykre konsekwencje.

9. Nie blokuj wszystkiego. Pracownicy w dzisiejszych czasach potrzebują dużo swobody online, aby móc efektywnie pracować. Zablokowanie wszystkiego zachęca pracowników do znalezienia "tylnej furtki". Porozmawiaj z nimi, dowiedz się czego chcą i pomyśl jak im to dać w jak najbezpieczniejszy sposób.

10. Uważaj na nośniki danych. Bardzo łatwo zostawić laptopa czy telefon bez opieki. Dane zawsze powinny być szyfrowane, ale należy też pamiętać o możliwości zdalnego wyczyszczenia urządzenia, gdy je utracimy.

** Sophos przeprowadził badanie w czerwcu i lipcu 2010*

Sophos