

## Firmowe komputery - w ogniu walki.

W świecie cyfrowym trwa odwieczna walka dobra ze złem. Po jednej stronie wirusy, robaki, konie trojańskie, szpiegdy i cała reszta, po drugiej - antywirusowe szczepionki, zapory ogniowe i cała reszta strażników. A w ogniu walki - my i nasze firmowe komputery.

W firmach z sektora MSP, które mają większe ograniczenia budżetowe, wydatki na rozwiązania z zakresu bezpieczeństwa muszą być bardzo przemyślane. Dobrze zdefiniowana polityka bezpieczeństwa firmy pozwoli nie tylko jasno określić zakres procesów objętych zabezpieczeniami antywirusowymi czy antyphishingowymi, ale także skutecznie przeciwdziałać potencjalnym zagrożeniom.

Przy formułowaniu zasad polityki bezpieczeństwa warto uwzględnić: konieczność ciągłej i częstej aktualizacji stosowanych zabezpieczeń, potrzebę integracji systemów zabezpieczających dwa różne środowiska (np. sieci WLAN i hurtowni danych, świadomość, że celem

systemu jest minimalizacja ryzyka utraty informacji - żaden system nie jest w 100 proc. bezpieczny, oraz ludzi - jako najłabsze ogniwo całego procesu.

W małej firmie, gdzie większość danych przechodzi przez ręce właściciela, warto wdrożyć rozwiązanie umożliwiające szybki dostęp do kluczowych informacji, ale chronionych przez wielostopniowy system zabezpieczeń. Całość prac związanych z utrzymaniem infrastruktury i aktualizacją oprogramowania można powierzyć firmie outsourcingowej.

**Adam Gębski**

---

ZETO S.A.