Luki w systemach IT – pierdyliardy kodu i małe kwiatki

W świecie IT często mówi się o bezpieczeństwie w kategoriach wielkich mechanizmów: SPF, DKIM, DMARC, szyfrowanie end-to-end, miliardy linii kodu zabezpieczających serwery pocztowe i aplikacje. Tworzy to obraz hermetycznego systemu, w którym nic nie ma prawa się wydostać. A jednak...

Gdzie rodzą się luki?

Najczęściej nie w samych algorytmach kryptograficznych czy protokołach, ale w tym, co **najbardziej ludzkie**: - ktoś kiedyś dodał alias, by przekierować pocztę na prywatny adres, - zapomniano o starym wpisie w konfiguracji, - serwer generuje komunikat błędu i „mimowolnie" zdradza coś, czego nie powinien.

Iluzja szczelności

Bezpieczeństwo IT to nie tylko potężne mury, ale też setki małych furtek. Możesz mieć najbardziej zaawansowane protokoły uwierzytelniania, a i tak system „wypapla" informację w nagłówku zwrotki. To pokazuje, że **pierdyliardy linijek kodu nie chronią przed drobiazgami**, które powstają na styku człowieka i maszyny.

Dlaczego to ważne?

Bo większość „wycieków" nie wynika z genialnych ataków hakerskich, tylko z: - drobnych przeoczeń, - nieusuniętych wpisów, - niewłaściwie skonfigurowanych usług.

To jest właśnie ironia: technologia potrafi być potężna, ale **najbardziej zdradza nas rutyna**.

Wnioski

1. Systemy są tak mocne, jak ich **najsłabsze ogniwo** – a tym zwykle jest człowiek.
2. „Wielkie zabezpieczenia" mogą paść przez mały, stary wpis w konfiguracji.
3. Żaden system nie jest absolutnie szczelny – i to nie wada, ale przypomnienie, że **trzeba myśleć krytycznie o technice**.

Tak powstają kwiatki w stylu: miliardy wydane na bezpieczeństwo, a system i tak ujawni coś, co miał ukryć. To dobra lekcja pokory wobec technologii – i świetne przypomnienie, że w IT nie ma świętych krów.