Kybernetická bezpečnosť

HROZIVÉ FAKTY

Následujúce varovné údaje vyplývajú zo serióznych prieskumov z rokov 2012-2016 týkajúcich sa kybernetickej bezpečnosti. Uvidíme, ako sa situácia v Európe zlepší s prijatím nariadenia GDPR. V každom prípade je zjavné, že otázka IT bezpečnosti bude s nárastom internetu vecí čím ďalej aktuálnejšia.

Mnoho dát unikne preto, pretože firmy neaplikujú bezpečnostné záplaty.

85% úspešných útokov mierilo na 10 najznámejších zraniteľností, ktoré neboli odstránené, aj keď boli záplaty k dispozícii

83% obetiam útokov trvalo dlhšie než týždeň, kým únik dát detekovaly

Zdroj: CompTIA, „Trends in Information Security," 2015

Najviac kyberútokov je vedených interným zamestnancom

60% Kybernetických útokov v roku 2015

44.5% sa považuje za „veľmi škodlivých"

Zdroj: IBM: „2016 Cyber Security Intelligence Index"

Mnohým bezpečnostným chybám sa dá jednoducho predísť

42% jednotlivcov uviedlo, že na vine bolo jednanie koncového užívatela ktorý, nedodržoval predpisy

Mnoho organizácií nemá plán pre zabezpečenie ich IT bezpečnosti

43% výkonných manažérov si myslí, že majú efektívnu stratégiu pre IT bezpečnosť

Zdroj: PWC: „Cybersecurity: The new business priority," 2012

2/3 manažérov CIO a CISO vraví, že ich spoločnosti nevnímajú kybernetickú bezpečnosť ako prioritu

Zdroj: „2015 Global Megatrends in Cybersecurity," Ponemon Institute LLC. (conducted for Raytheon)

Vzostup IoT vzyšuje bezpečnostné hrozby

70% zariadení IoT nieje dostatočne zabezpečených pred útokmi

Zdroj: „Internet of Things State of the Union Study," 2014

Vaši zamestnanci potrebujú poznať riziká

Lepšie povedomie zamestnancov o spôsoboch , ako zabezpečiť kyberbezpečnosť spôsobí **30%** pokles bezpečnostných rizík

Zdroj: „2015 Global Megatrends in Cybersecurity," Ponemon Institute LLC. (conducted for Raytheon)

Mnoho SMB firiem podceňuje kybernetické hrozby

77% SMB firiem tvrdí, že ich spoločnosť je zatial voči útokom chránená

83% z nich nemá formálny bezpečnostný plán

Zdroj: National Cyber Security Alliance (NCSA) and Symantec

Top 10 doporučení od spoločnosti AXIS Communications ako zabezpečiť kybernetickú bezpečnosť

Väčšine kybernetických útokov a prípadov zneužitia kamier sa dá predísť s pomocou niekoľkých základných krokov.
Na webovej stránke **www.axis.com** pri zadaní hesla Cybersecurity nájdete súhrn všetkých dôležitých informácií k tejto téme vrátane podrobného manuálu Axis Hardening Guide pre zabezpečenie kamier.

Tu uvádzame 10 najdôležitejších tipov pre správcov kamerových systémov alebo systémových integrátorov.

1

Vytvorte analýzu rizík vzhľadom na potenciálne hrozby a možné škody, keby došlo k napadnutiu systému.

2

Získajte vedomosti o ochrane systému a možných hrozbách.
Úzko spolupracujte s predajcami, systémovými integrátormi, konzultantmi, výrobcami produktov.
Internet je fantastický zdroj informácií.

3

Zabezpečte sieť.
Keď je narušená sieťová ochrana, zvyšuje sa riziko úniku citlivých informácií a útoku na jednotlivé servery alebo sieťové zariadenia.

4

Používajte silné, unikátne heslá a v pravidelných intervaloch ich meňte.

5

Nespoliehajte na prednastavené továrenské nastavenia daného produktu:

- Zmeňte prednastavené heslo
- Nakonfigurujte pre zariadenie ochranné služby
- Vypnite služby, ktoré sa nepoužívajú

6

Pokiaľ je to možné, používajte šifrované pripojenie, a to aj na lokálnych sieťach.

7

Pre zníženie rizika, že bude zneužité video, by klienti nemali mať priamy prístup ku kamere, ak to systém či riešenie nevyžaduje.
Klienti by mali k videu pristupovať iba cez VMS (Softvér pre správu videa) alebo media proxy server.

8

Pravidelne kontrolujte prístupové logy, aby ste podchytili pokusy o neautorizovaný prístup.

9

Pravidelne monitorujte zariadenia.
Zapnite systémové notifikácie, ak sú potrebné a sú podporované.

10

Používajte posledný dostupný firmware, pretože môže obsahovať bezpečnostné záplaty.