ONLINE BEZPEČNOSŤ PRE VÁS A VAŠU SPOLOČNOSŤ

PLUG IT

DOMINIK BRANIŠA

OBSAH.

- VEDELI STE, ŽE?
- MÁLO INFORMÁCII
- MANAŽMENT PRÍSTUPOV
- NEDOSTATOČNÉ ZÁLOHOVANIE
- STARÉ VERZIE SYSTÉMOV
- SLABÉ HESLÁ

VEDELISTE ŽE?

- 46% z celkového množstva hackerských útokov je zameraných na malé a stredné spoločnosti
- 47% z týchto útokov bol ransomware, 73% postihnutých spoločnosti zaplatilo výkupné
- Priemerná ročná strata spôsobená týmito útokmi je až 23 626 €
- Iba 14% je pripravených na takýto útok
- 95% percent všetkých prienikov je spôsobených ľudským faktorom?

Práve kvôli tomu vám prinášame zoznam 5 vecí, ktoré priamo ohrozujú bezpečnosť vašich dát, ale hlavne aj odporúčania, ktoré viete aplikovať prakticky okamžite, zadarmo a zvýšiť tým úroveň bezpečnosti vo vašej spoločnosti.

MÁLO INFORMÁCIÍ

Jeden z najdôležitejších bodov, na ktoré by ste mali vo firme dbať, ak nechcete dáta zbytočne vystavovať ohrozeniu, je vzdelaný personál.

Sú to práve ľudia, ktorí sú častokrát najslabším článkom v reťazci a kvôli ktorým firmy prichádzajú o dáta. Dajte si preto záležať, aby ľudia vo vašej firme boli pravidelne školení ohľadom online bezpečnosti a poznali aktuálne trendy.

Dodnes sa stáva, že zamestnanci vo firmách otvoria podozrivú prílohu či nekontrolujú, od koho dostali email a vystavia tak firemné dáta riziku. Dá sa tomu ľahko predísť.

MANAŽMENT PRÍSTUPOV

Je úplne bežnou praxou, že v rámci všetkých systémov a nástrojov, ktoré sa vo firme používajú, má majiteľ prístup ku všetkému a má všetky právomoci.

Aj tam, kde to nie je potrebné. Práve toto robí z majiteľa veľmi atraktívny cieľ pre hackerov, ktorým tak stačí dostať sa do počítača jednej osoby a získajú prístup k všetkým dátam.

Dajte si pozor, kto má vo firme k čomu prístup, a či ten prístup naozaj potrebuje.
Aj v prípade útoku na konkrétnu osobu tak bude riziko menšie, ako keby mal jeden človek prístup ku všetkému.

NEDOSTATOČNÉ ZÁLOHOVANIE

Kedy ste naposledy zálohovali firemné dáta? V tom lepšom prípade odpoviete, že dnes alebo včera, pretože viete, že sa to vo vašej firme deje automaticky a nemusíte na to myslieť.

V tom horšom prípade to robíte ručne raz za čas no a úplne najhorší scenár je, že sa to nedeje vôbec.
Bohužiaľ ten najhorší je aj najčastejší a pritom zálohovanie nie je žiadna jadrová fyzika.

V prípade útoku a zablokovania dát hackermi tak jednoducho zariadenie vymažete, obnovíte zo zálohy a fičíte ďalej.

STARÉ VERZIE SYSTÉMOV

Viete o tom, že aktualizácie jednotlivých aplikácií a operačných systémov okrem vylepšení a nových funkcií prinášajú aj opravy bezpečnostných nedostatkov?

Je to jeden z dôvodov, prečo by ste mali udržiavať vaše firemné zariadenia vždy aktualizované a používať najnovšie verzie dostupného softvéru.

V opačnom prípade budú zariadenia so starým verziami ľahkým terčom útokov hackerov.

SLABÉ HESLÁ

Viete, aké sú najčastejšie používané heslá v online priestore?
Pravidelne sa robia prieskumy, ktoré skúmajú používané heslá a na top priečkach sa obsadzujú stále tie isté prípady.

Či už je to 12345 alebo meno zvieraťa, či slovo “heslo,” všetko to otvára dvere hackerom.
Uhádnuť jednoduché heslo môže trvať niekoľko sekúnd a vaše dáta budú stratené.

Dajte si záležať na naozaj kvalitnom hesle. Využite nástroj na generovanie a ukladanie hesiel a ani si ich nebudete musieť pamätať.

ĎAKUJEME.

DOMINIK BRANIŠA

WWW.PLUGIT.SK

BRANISA@PLUGIT.SK

0910 906 668