Informaciona sigurnost ključna je stvar tokom životnog perioda Vaše kompanije

U posljednje vrijeme primjećen je značajan porast napada putem interneta, **cyber napada.**
Radi se ustvari o napadu na računarski uređaj sa zlonamjernim programima u cilju onemogućavanja njegovog korištenja, a sa druge strane nelegalnog sticanja koristi putem ucjenjivanja žrtava.

Tradicionalni "firewall" uređaji više nisu dovoljno efikasni u sprečavanju ovih napada.
Savremeno poslovanje nezamislivo je bez pristupa javnim mrežama i servisima - elektronsko bankarstvo, web prodavnice...
To povlači potencijalnu sigurnosnu prijetnju u vidu neautorizovanog pristupa izvana u lokalnu mrežu.

NG - Next Generation "firewall" nudi tradicionalnu zaštitu na nivou mrežnih adresa i protokola/portova, ali i sprečavanje upada (Intrusion Prevention), filtriranje web sao-braćaja (Web Filtering), "antimalware" i kontrolu aplikacija.
NG "firewall" dodatno pruža zaštitu za uređaje na koje se ne može instalirati "antimalware" (ruteri, switch-evi itd).

Napadi koriste slabosti i ranjivosti sistema sa ciljem ostvarivanja neautorizovanog pristupa, što ima za posljedicu:

- Zaključavanje uređaja, kao relativno jednostavan problem za rješavanje
- Kriptovanje podataka, kao veoma težak problem za rješavanje

Šta se dešava nakon napada?

Nakon što se onemogući pristup podacima na uređajima koji su „zaraženi“, obično se pojavljuje poruka sa tekstom u kojem se zahtjeva da se određeni iznos novca uplati na „njihov“ račun da bi se omogućio ponovni pristup podacima.

Ukoliko firma „žrtva“ nema ažuran backup podataka, jedino preostaje da se izvrši uplata navedenog novčanog iznosa.

U većini slučajeva, čak i nakon uplate navedenog novčanog iznosa, napadač ne omogućava pristup zaključanim podacima čime se dodatno povećava nastala šteta.

Kako Vam možemo pomoći?

Za zaštitu od ovakvih vrsta napada preporučujemo sljedeće:

Spriječiti zlonamjerni softver.
Instalirati kvalitetan, pouzdan i provjeren softver za zaštitu od zlonamjernog softvera.

Implementirati backup podataka.
Raditi backup važnih podataka na više lokacija, prvenstveno na eksterni medijum.

Kontrolisati i ograničiti pristup podacima.
Implementirati pristup prema principu „najmanjih privilegija“, ograničiti administratorski pristup.

Implementirati domenski režim rada u mreži.
Postaviti sigurnosna podešenja i centralizovano upravljati IT infrastrukturom.

Naš tim za IT infrastrukturu, sigurnost i kvalitet pruža usluge informacione sigurnosti uz primjenu savremenih tehnologija i primjenu proizvoda vodećih svjetskih kompanija (CISCO, Fortinet, Kaspersky, Microsoft, Veeam, Acronis).

JAVITE NAM SE

Imel
Since 1994

Skendera Kulenovića bb, 75300 Lukavac, Bosna i Hercegovina
Telefon: +387 35 550 100 *e-mail: it.podrska@imel.ba*
Fax: +387 35 553 503 *info@imel.ba*