KEND SÅRBARHEDERNE

– Bliv klogere på jeres netværkssikkerhed

Netværksinfrastrukturen i din virksomhed kræver konstant opmærksomhed, udvikling og tilpasning for at understøtte forretningens behov.

Samtidigt skal I tage hensyn til den stigende trussel fra avancerede angreb. Der er to måder at gøre dette på – proaktivt eller reaktivt.

Ved at tilegne jer viden omkring jeres nuværende trusselsbillede, kan I være proaktive.

Fortinet CTA – Cyber Threat Assesment, kan hjælpe jer med at forstå:

> Sårbarheder og trusler

Få information om trusler i jeres nuværende setup. Få oplysninger om eksisterende exploits, og få en gennemgang af jeres enheder, og hvilke der er specielt sårbare over for angreb.

> Brugerproduktivitet

Hvilke peer-to-peer, sociale medier, IM og andre applikationer kører på jeres netværk – og hvem der bruger hvad.

> Netværksforbrug og performance

Hvad bliver netværket brugt til, hvad presser sikkerheden, kan intelligens erstatte råstyrke.

Kontakt

Dennis Larsen
Salgsdirektør
dbl@businessmann.dk
+45 2427 1411

Fortinet CTA krav hos jer:

- ✓ Adgang til en SPAN port i jeres core switch.
- ✓ Adgang til internet – så enheden kan opdatere.
- ✓ Brug af Sandbox*, vi anbefaler en internetadgang på en separat forbindelse.
- ✓ Enheden skal sidde i 14 dage med et almindeligt driftsmønster.
- ✓ Enheden vil være transparent for jeres brugere.
- ✓ Evt. mulighed for integration med jeres interne Directory Service til bruger genkendelse.

Fortinet CTA forløb:

1. Designmøde, opstilling af mål for processen.
2. Enheden bliver installeret og konfigureret hos jer.
3. Vi verificerer at løsningen er klar til datalogning, uden at den forstyrrer driften.
4. 14 dage senere afhenter vi boksen, og verificerer driften er stabil.
5. 7 dage senere fremlægger vi vores opdagelser for jer.
6. Implementering af anbefalinger.

(*) Sandbox er en service der eksekverer ukendte filer i et virtuelt og lukket miljø for at finde ud af om det er Malware.