Et godt cyberforsvar

De 7 vigtigste værktøjer

Mentor it
- med dig i fremtiden

Ingen kan sikre sig fuldstændigt mod de trusler, der kan ramme en virksomheds IT-systemer. Alt er muligt og ingen mure er høje eller kraftige nok til at forhindre uønskede sikkerhedshændelser.

Selvom oddsene er svære, er der en række tiltag, der i høj grad bidrager til et godt cyberforsvar. Både før, under og efter en sikkerhedshændelse. Vi har samlet de 7 vigtigste værktøjer lige her.

God læselyst.

1

Planlægning

Forberedelse er altafgørende, når det kommer til at identificere, forhindre og håndtere mulige trusler.

Eksempler på værktøjer hertil er risikovurdering, beredskabsplan og recovery plan. Altså strategiske overvejelser omkring, hvordan du forholder dig til risicis, sikkerhedsforanstaltninger og handling, hvis skaden sker.

I en krisesituation, som et cyberangreb eller en kritisk sikkerhedshændelse typisk vil være, er det en kæmpe hjælp og sikkerhed, at handlingsplaner herfor allerede eksisterer.

Har du ikke læst de opmærksomhedspunkter, som Per Silberg Hansen fra Improsec tidligere har fremhævet, netop i forhold til god forberedelse, er de fortsat meget relevante. Du kan finde dem her.

Logning

Logning gør det muligt at spore og identificere aktiviteter i ens systemer. En klar nødvendighed, hvis der opstår tvivl om, hvorvidt nogen lusker uhensigtsmæssigt rundt i netværket, eller hvis der er behov for at identificere og inddæmme en trussel, virus eller uønsket gæst.

Rammes virksomheden af et cyberangreb, kan logning være helt afgørende i forhold til at dokumentere og redegøre for den konkrete situation. Sidstnævnte er ofte særlig vigtig både i forhold til datatilsynet og forsikring.

Center for Cybersikkerhed har netop opdateret deres vejledning omkring logs. Find den her.

Nedenfor finder du fire specifikke grunde til, at logning er vigtigt.

Derfor er logning *vigtigt*

- Basis for at undersøge et cyberangreb
- Mulighed for at kende omfanget af et cyberangreb
- Mindre nedetid i forbindelse med cyberangreb
- Viden om normalbilledet i netværket

3

Backup

Backup er afgørende i forhold til at komme tilbage til normal drift, hvis data slettes forsætligt eller ved fejl. Det kan være i forhold til mindre ting, men det kan også være, hvis virksomheden rammes af et cyberangreb. Her vil en backup spille en afgørende rolle for virksomhedens eksistens og mulighed for at komme tilbage til normal drift.

Backup kan være et vidt begreb og bør uden tvivl være et vigtigt punkt både i forhold til risikovurdering, beredskabsplan og recovery plan.

Backup bør altid etableres på mindst 2 forskellige og adskilte backupteknologier, da backup også kan kompromitteres.

Som eksempel er det ofte nødvendigt at tage backup af flere ting, definere rammen for backups og sidst men ikke mindst: Have en offline backup, som ikke er en del af dit eget system.

Brugersikkerhed

Ingen er stærkere end det svageste led, og dine medarbejdere er en vigtig del af sikkerhedskæden, når det kommer til din IT. Vi ved fra statistikker, at størstedelen af de sikkerhedshændelser, der udspiller sig, starter hos medarbejdere.

Det kan være en bruger, der kommer til at klikke på et forkert link eller dele fortrolig information. Det er nemt at blive narret, og derfor enormt vigtigt, at virksomheden gør sit yderste for at skabe en tryg og sikker arbejdsplads, hvor medarbejderne indgår som et proaktivt værn mod sikkerheds-trusler.

Brugersikkerhed er som eksempel: Tofaktor-godkendelse, awareness træning, passwordpolitikker og kendt IT-/sikkerhedspolitik. Værktøjer, som generelt højner sikkerheden omkring brugernes adgang og ageren til og i virksomhedens systemer.

Netværkssikkerhed

Virksomhedens netværk er en direkte indgang til systemer og infrastruktur, og hvis sikkerheden ikke er i top, er netværket også en direkte indgang for udefrakommende. Særligt fem punkter spiller en væsentlig rolle, når det kommer til et sikkert netværk:

1. Opdaterede firewalls

Er en firewall ikke opdateret eller konfigureret korrekt, overvåges og defineres trafikken hverken optimalt eller sikkert. Dette gælder både for software og firmware.

2. Gæstewifi

Et gæstenetværk kan være en direkte adgang for udefrakommende til virksomhedens infrastruktur, hvis opsætningen ikke er konfigureret korrekt.

3. Netværkssegmentering

Et netværk bør tilpasses de forskellige klienter, der tilgår, så trafikken er kontrolleret og segmenteret. Gælder eksempelvis printere, telefoni og produktion.

4. Fysisk sikkerhed

Det er vigtigt at sikre sit netværksudstyr, så udefra- eller uvedkommende ikke kan tilgå og opnå utilsigtet adgang.

5. Tilknyttede sikkerhedslag

De udvidede services, som giver mening, bør tilføjes netværket. Dette kan være webfiltrering, antivirus detection, anti-malware detection, geoblocking, intrusion prevention osv.

Opdatering

Styresystemer og applikationer skal være opdateret for ikke at udgøre en potentiel risiko for virksomhedens sikkerhed. Det kan for eksempel være Windows OS eller de programmer, du dagligt benytter til at udføre dit arbejde.

Er disse ikke opdateret, kan der opstå sikkerhedshuller, som ikke automatisk bliver lukket og små indgange til virksomhedens infrastruktur opstår dermed.

For at sikre løbende opdatering heraf, giver det mening at advisere omkring disse og allerbedst:
Sikre automatisk udrulning af opdateringer.
For eksempel igennem Intune.

Løbende status

IT-sikkerhed skal genbesøges. Virkningen af en indsats er ofte midlertidig og kræver løbende vedligeholdelse, ligesom nye trusler hele tiden opstår og skal håndteres.

Du kan sikre løbende fokus på din sikkerhed ved at planlægge statusmøder med din trusted advisor, genbesøg og vedligeholdelse af den sikkerhedsplan, der eksisterer samt opfølgning på de sikkerheds-scores, som virksomheden har/får.

Brug for mere vejledning?

Vores sikkerhedsspecialister og dygtige rådgivere hjælper dig gerne videre, hvis du har spørgsmål eller brug for hjælp til de 7 væsentlige værktøjer til et godt cyberforsvar.

Kontakt din nærmeste kontaktperson ved Mentor IT eller **ring 70 122 123.**

Mentor IT Esbjerg

Mentor IT Kolding

Mentor IT København

Mentor IT Aarhus

Telefon +45 70 122 123

E-mail info@mentor-it.dk

Mentor it

– med dig i fremtiden