# Kommentarer – Grundläggande it-säkerhetsåtgärder – en vägledning - förhandsutgåva

## Namn: Säkerhets- och försvarsföretagen, SOFF (www.soff.se)

| ID | Identifierad förbättringsmöjlighet | Förslag på hur detta kan lösas | Kommentar | Omhändertaget på vilket sätt |
|---|---|---|---|---|
| | **Övergripande** | | | **(Kolumnen ifylls av MSB)** |
| **1** | Information om vilken hotbild säkerhetsåtgärderna är dimensionerade mot. | Beskriv vilken typ av hotaktörer som säkerhetsåtgärderna bedöms skydda mot alternativt gruppera att en viss mängd av åtgärder uppnår skydd mot en viss typ av hotaktörer, och ytterligare kontroller mot en viss typ. | | |
| **2** | Lösenordslängd (sid 28) beskrivs bara som unika, långa och starka. Här önskas en definition av vad detta innebär. | Borde ha minsta längd 15 tecken (20 för systemadminkonton). | | |
| **3** | Proxy (Secure Web Gateway) | Lägg mer vikt vid betydelsen av en vad en riktig proxy faktiskt innebär.<br>- Att inte användarna och deras enheter exponeras direkt mot internet (helt olika tcp-koppel).<br>- Att man då kan scanna all trafik med Anti Malware, Machine Learning samt full Sandboxing (beroende på val av lösning såklart)<br>- Att man upprätthåller en hög säkerhet för SSL/TLS (baserat på stort stöd för de cipher suites som | Tydligare rekommendation för organisationer med höga säkerhetskrav. | |

| | | | | |
|---|---|---|---|---|
| | | rekommenderas och faktiskt används).<br>- Brandväggar (NGFW) streamar paket och kan aldrig få en lika klar uppfattning av ”helheten” utan proxyfunktionalitet, de nedgraderar dessutom ofta valet av cipher suite pga. att de ej har stöd/för att det tar för mycket prestanda.<br>Genom att låta samtlig webbtrafik gå genom en proxy kan man dessutom stoppa IoT relaterade hot när en enhet försöker nå sin Command and Control server. | | |
| **4** | Löpande IT-/Informationssäkerhetsutbildning för samtliga medarbetare | Detta bör alla organisationer göra löpande. IT-/Informationssäkerhet samt phishingtester. | Kan ställa krav på att leverantören har personal med it-säkerhetskompetens vid utkontraktering och arbetar med löpande kompetenshöjande utbildning. | |
| **5** | MITRE ATT&CK™ | Lägg till någon referens till MITRE ATT&CK™ i dokumentet. | | |
| **6** | Loggning: loggar som ska användas forensiskt MÅSTE säkerställas att de inte är manipulerade, annars faller stora delar | Förtydliga dokument runt området loggning. | | |

| | | | | |
|---|---|---|---|---|
| | av bevisvärdet i en eventuell juridisk aspekt. | | | |
| **7** | Gemensam tid: Rekommendera att man har gemensam tid i systemet, och inte bara hänvisar till 2 olika källor. Det är bra för att synka mot en omvärld, men internt blir det onödigt svårt och tidsödande om man tillåter flera källor. | Förtydliga dokument i området runt tid. Förslag är att använda den tid som produceras i Sverige av NetNod, PTS och Sveriges tekniska forskningsinstitut SP i Borås. | | |
| **8** | Stora delar av mottagarna (myndigheter, kommuner, landsting mm) bör fundera över olika givna författningar som kravställer och det nämns bara i en punkt (1.1.5, sidan 11). Där kommer nämligen all formell lagstiftning in. | Förtydliga dokument runt området runt kravställan. | | |
| **9** | I övrigt en mycket bra vägledning, den kommer att vara till stor hjälp för många framöver. | | | |