MYNDIGHET 459 FÖR SÄKERHETSNÖRDAR

För dig som jobbar med IT, säkerhet eller människor som använder IT

Här finns VPN, kryptering, digital forensik, insiders, social engineering, loggar, underrättelsearbete, säkerhetsskåp och ett USB-minne som väldigt många människor vill kontrollera.

Men det här är **inte ett quiz i att hitta säkerhetsfel.**

Använd i stället boken som ett gemensamt scenario. **Välj 5–7 frågor som lockar.** Börjar någon berätta om ”en organisation jag absolut inte tänker namnge…” är ni sannolikt på rätt spår.

Spoilervarning: Frågorna förutsätter att alla har läst hela boken.

BÖRJA HÄR

Vilken säkerhetsscen fick dig mest att tänka: ”Det där skulle absolut kunna hända hos oss”?

Berätta gärna varför. Utan att nämna arbetsgivaren, om det känns klokast.

MÄNNISKAN: PROBLEMET ELLER SUPERKRAFTEN?

1. Du får rekrytera en person från Myndighet 459 till ett red team. Vem tar du?

Vilken av personens ”dåliga” egenskaper är egentligen precis den kompetens du vill åt?

2. Vilka attacker i boken fungerar just därför att människor beter sig normalt, inte därför att de är dumma?

Hjälpsamhet? Konflikträdsla? Attraktion? Auktoritet? Skam? Lydnad? Nyfikenhet? Något annat?

NÄR SÄKERHET MÖTER VERKLIGHETEN

3. Ni är CISO hos polisen och upptäcker Malte först efteråt. Vilken kontroll inför ni på måndag?

Och vilken kontroll vägrar ni införa eftersom den skulle göra forensikernas riktiga arbete orimligt svårt?

4. Malte använder VPN, Protonmail och Bitcoin men kopplas ändå till utpressningen genom andra spår.

Vad krävs egentligen för att vara anonym?

Och när är en attribuering på ungefär 80 procent tillräckligt bra för att man ska agera?

5. Vera gör nästan allt ”rätt”, men ett enda missat VPN-tillfälle skapar ett avgörande spår.

Är säkerhet som kräver att människor aldrig gör fel egentligen säker?

6. Vilken säkerhetskontroll i boken skulle lätt kunna få grönt i en revision och ändå vara nästan värdelös när någon faktiskt försöker angripa systemet?

Försvara gärna ert val.

7. Partiets loggsystem fungerar precis som organisationen har beslutat, och därför är den gamla bevisningen borta.

Är det ett säkerhetsfel, ett styrningsfel eller ett system som fungerar perfekt mot fel mål?

Och hade mer loggning automatiskt varit bättre?

8. Signal är korrekt konfigurerat. Sedan kommer kattbilderna och memesen.

Vad löser säker teknik, och vad löser den inte?

EN OBEHAGLIGT REALISTISK FÖLJDFRÅGA

Efter en sådan incident, vad skulle er egen organisation troligast göra?

A. Ändra tekniken
B. Ändra processen
C. Skriva en ny policy
D. Boka obligatorisk utbildning för samtliga anställda

Försök gärna försvara svaret.

INFORMATION, ANSVAR OCH MAKT

9. Bob undanhåller information för att få gruppen att göra det han behöver.

Är det säkerhetsledning eller manipulation?

Var hade du själv dragit gränsen?

10. USB-minnet byter händer flera gånger. Vem i boken är egentligen farligast att ge det till, och vem skulle du själv lita mest på med det?

Vad är det som gör informationen farlig: innehållet, personen som förstår den eller personen som faktiskt kan använda den?

11. När Chefen till slut får USB-minnet, är operationen lyckad, eller har hotet bara fått en ny ägare?

OM NI VILL NÖRDA NER ER LITE TILL

Vem i boken skulle du vara allra mest nervös över att ge admin-rättigheter? Försvara ditt svar.

Om du fick göra en enda säkerhetsförändring i hela romanens värld, vilken skulle ge störst faktisk riskreduktion?

FORTFARANDE OENSE?

Marcus Nohlberg forskar och föreläser om informationssäkerhet, social manipulation och mänskligt beteende.

Om ni har diskuterat färdigt och fortfarande vill argumentera kan Marcus, kostnadsfritt och i mån av möjlighet, ansluta digitalt i cirka 20–30 minuter för frågor om säkerheten, researchen, verklighet kontra fiktion eller era egna slutsatser.

Kontakt och mer information: myndighet459.se