Tabletop-övning för nätfiske

CERT-SE

2026-04-07

Tabletop-övning – Nätfiske (phishing) för [er organisation] [datum för genomförande] [övningsledare] [deltagare]

Syfte

Syftet med den här övning är enligt följande:

- Träna på hantering och beslutsfattande kring IT-säkerhetsincident (Nätfiske).
- Höja medvetenheten kring organisationernas olika roller i incidenthanteringen.
- Identifiera förbättringsområden för att stärka cybersäkerheten i er organisation.
- Beakta krav enligt NIS2-direktivet och cybersäkerhetslagen och/eller annan lagstiftning/certifiering som styr just er verksamhet.

Instruktioner till övningsledaren
Förberedelse: 10 minuter. Alla deltagare läser igenom detta dokument. Dela in deltagarna i roller (Se tabellen nedan för exempel på roller). Tänk på att fördela ordet jämt och att alla ska få komma till tals.

Genomförande: 30 minuter. Läs upp scenariot och gå igenom fas 1, 2 och 3 stegvis. Avbryt inte diskussionerna men om samtalen inte uppfyller syftet, stötta med att inrikta diskussionen. Diskutera frågorna utifrån era roller och er organisation.

Utvärdering: 10 minuter. Observera spelarna, notera besluten och riskidentifieringen som lyfts fram. Dokumentera konkreta förbättringsåtgärder. Avsluta och utvärdera enligt mall.

Förslag på roller

Roll	Ansvar / Funktion
Övningsledare	Leder övningen, tar anteckningar
VD / Ledning	Beslutar om strategi, resurser och rapportering
IT / Drift / Säkerhetschef	Ansvarar för teknik, backuper och incidenthantering
Juridik / Informationssäkerhetsansvarig	Ansvarar för regelefterlevnad exempelvis NIS2, Cybersäkerhetslagen
Kommunikation / PR	Ansvarar för intern och extern kommunikation
Verksamhetsrepresentanter	Definierar affärskritiska processer och prioriteringar

Scenario
En morgon får flera medarbetare ett mejl som ser ut att komma från organisationens ekonomiavdelning. Mejlet uppmanar mottagaren att snabbt bekräfta en faktura via en länk, eftersom ”betalningen annars inte går igenom”.

Kort därefter rapporteras det om ovanlig aktivitet hos ett användarkonto.

Fas 1: Initial analys
Vad är era första reaktioner?
Vilka omedelbara åtgärder vidtar ni första timmen?
Hur identifierar ni att det kan röra sig om nätfiske eller bedrägeriförsök?
Har ni en incidenthanteringsplan? Kan ni era rutiner? Har ni rätt resurser?
Vilka loggar har ni tillgång till och hur långt tillbaka sträcker sig loggarna?

Fas 2: Åtgärder och strategi
Hur rapporterar medarbetare misstänkta e-postmeddelanden idag?
Vilka tekniska och organisatoriska skydd finns på plats (t.ex. multifaktorautentisering, e-postfilter, utbildning)?
Hur kommunicerar ni internt och externt vid misstänkta eller pågående nätfiskeangrepp?
Vilka juridiska krav gäller enligt NIS2 och cybersäkerhetslagen?
Behöver händelsen rapporteras till myndighet (exempelvis CERT-SE enligt NIS2)?
Vem gör polisanmälan?

Fas 3: Åtgärder och strategi
Vilka lärdomar kan ni dra från detta scenario och vilka förbättringsåtgärder behövs?
Vad kan ni göra för att förhindra att det händer igen?

Avslutning och utvärdering
Diskutera följande: Hur tyckte ni att övningen gick? Vad borde göras annorlunda om det hände i verkligheten? Lärde ni er något?

Håll fokus på att deltagarna identifierar brister i nuvarande rutiner och konkreta förbättringsförslag. Dokumentera förslag och ansvarsfördelning för uppföljning. Sammanfatta och ge konkreta förbättringsförslag (Se nedan för förslag på mall).

Förslag på mall:

Identifierad brist eller risk	Åtgärd	Resurser	Ansvarig och tidsplan