Tabletop-övning för utpressningsangrepp

CERT-SE

2026-04-07

Syfte

Syftet med den här övning är enligt följande:

- Träna på hantering och beslutsfattande kring IT-säkerhetsincident (Utpressningsangrepp).
- 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.

Tabletop-övning – Utpressningsangrepp för [er organisation]
[datum för genomförande] [övningsledare] [deltagare]

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 vanlig dag på jobbet. En av era medarbetare upptäcker att ärendehanteringssystemet eller liknande system är otillgängligt. Ni upptäcker att stora delar av filservrar och databaser är krypterade. Flera system går inte att använda. En hotaktör kräver en lösensumma via mejl och hotar att publicera data om inte betalningen görs inom 48 timmar. Kunddata/personuppgifter är i riskzonen. Verksamheten står stilla. Klockan tickar.

Fas 1: Initial analys
Vilka omedelbara åtgärder vidtar ni första timmen?
Har ni en incidenthanteringsplan? Kan ni era rutiner? Har ni rätt resurser?
Har ni en lista över prioriterade system? Vem beslutar om det? Hur lång är er faktiska acceptabla nertid för respektive system?
Vilka osäkerheter behöver ni utreda?
Överraskning: Backupservrarna är också krypterade.

Fas 2: Åtgärder och strategi
Vilka tekniska och organisatoriska motåtgärder aktiveras?
Hur organiserar ni intern och extern kommunikation?
Vilka juridiska krav gäller enligt NIS2 och cybersäkerhetslagen?
Behöver händelsen rapporteras till myndighet (exempelvis CERT-SE enligt NIS2)?
Hur tänker ni kring lösensumma och kommunikation med angriparna?
Vem gör polisanmälan?

Fas 3: Återställning och lärande
När och hur återställer ni system från backup? Vad gör ni om inte det går?
Hur säkerställer ni att angriparen inte ligger kvar?
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