Tabletop-övning för överbelastningsangrepp

CERT-SE

2026-04-07

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

Syftet med den här övning är enligt följande:

- Träna på hantering och beslutsfattande kring IT-säkerhetsincident (överbelastningsangrepp).
- 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 förmiddag upplever verksamheten kraftig försämring av tillgängligheten till webbtjänsten som kunder använder. Kundsupporten får in klagomål, och IT ser ovanligt hög trafik från okända IP-adresser. Kort därefter rapporterar driftleverantören misstänkt DDoS-aktivitet mot organisationens publika IP. Samtidigt får ni mejl från en okänd avsändare som påstår sig kunna avbryta attacken mot betalning i kryptovaluta. Verksamheten påverkas. Dessutom har journalister börjat höra av sig och ställer frågor. Tiden går.

Fas 1: Initial analys
Hur upptäcker ni att en DDoS-attack pågår?
Har ni övervakningssystem på plats?
Har ni en incidenthanteringsplan? Kan ni era rutiner? Har ni rätt resurser?
Vilka kontaktvägar har ni till er internetleverantör eller driftpartner vid incidenter?

Fas 2: Åtgärder och strategi
Har ni en eskaleringsrutin? Vem fattar beslut om att eskalera och till vem?
Överväger ni att betala den okända avsändaren för att attacken ska upphöra?
Vilken kommunikation sker internt och externt (t.ex. till kunder, leverantörer)?
Hur prioriteras tjänster? Vad är mest kritiskt att hålla igång?
Vem gör polisanmälan?

Fas 3: Återställning och lärande
Hur verifierar ni att attacken är över och att system är stabila?
Hur analyseras händelsen? Dokumenteras den?
Behöver händelsen rapporteras till myndighet (exempelvis CERT-SE enligt NIS2)?
Vilka tekniska och organisatoriska åtgärder kan vidtas för att förhindra liknande händelser? (Exempelvis CDN, rate limiting, redundans, leverantörskrav)
Hur kan ni stärka leverantöravtal för att säkerställa tillräckligt skydd och tillgång data för analys (loggar med mera).

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