48 dagar

Krisövning: cyberattack

Riksarkivet

Krisövning i att hantera en cyberattack

Alla kan drabbas av cyberattacker – mot de egna IT-systemen, en leverantör, ett datacenter eller någon annan man är beroende av.

Vid en allvarlig cyberattack kan det ta lång tid innan verksamhetens IT-infrastruktur fungerar igen.
Från ett par dagar till ett par månader!

Vad gör vi om det händer oss?

Varför gör vi den här krisövningen?

Syftet är skapa medvetenhet om risken för cyberattacker och få igång diskussioner om vad vi gör om vi drabbas.

Övningen genomförs i gruppdiskussioner där ni ska identifiera:

- Krishantering i det akuta inledningsskedet och den långa tid det tar innan krisen är över.
- Vad behövs för att vi ska kunna fortsätta bedriva verksamhet under pågående kris?
- Behov av förberedelser – vad borde ha varit på plats innan krisen inträffade?

48

DAGAR

Riksarkivet

Krisövning i att hantera en cyberattack

Scenariot i krisövningen bygger på cyberattacken som drabbade British Library i oktober 2023. Konsekvenserna av cyberattacken i scenariet är extrema, men inte osannolika.

Vill du veta mer, läs rapporten om cyberattacken mot British Library : *Learning lessons from the cyber-attack. British Library cyber incident review, 8 march 2024*

Riksarkivet

Scenario dag 1

- Besökare klagar över att våra digitala resurser inte fungerar. Databaserna går inte att nå, det går inte att göra beställningar.
- Webbplatsen ligger nere … och strax också intranätet.
- E-posten har också lagt av. Alla system verkar ligga nere!
- Det går inte att nå nätverket och inte att komma åt några filer. Har vi inte ens någon internetuppkoppling?
- Och nu fungerar inte telefonerna längre!

Efter ett par timmar fungerar varken datorer eller telefoner. Vad är det som har hänt?

Zero-day attack och ransomware

Vårt scenario: Med hjälp av MSB konstateras att hackergruppen **BioHaz** har utfört en zero-day attack. Ännu har inte någon lösensumma begärts!

- Cyberattacker sker genom att angriparen hittat en sårbarhet i ett IT-system som går att använda för att skicka in skadlig kod.
- En zero-day attack är när angriparen utnyttjar en sårbarhet som inte tidigare är känd – det tar tid att analysera det som hänt och hitta lämpliga åtgärder. Ungefär som att det tar tid att skapa ett vaccin när en ny sjukdom upptäckts.
- En attack med ransomware kan se ut på olika sätt, men vanligt är att data krypteras, nätverk och datorer förstörs och en lösensumma krävs för att inte den stulna informationen ska säljas eller publiceras på darknet.

Vad blir konsekvenserna av cyberattacken som drabbat oss?

- Verksamhetens datorer och mobiler har blivit förstörda och kommer inte att kunna användas igen – all utrustning måste bytas ut.
- Vissa datorer och mobiler har varit avstängda och är ännu ej smittade. De behöver ett uppdaterat antivirusprogram innan de kan sättas på – annars händer samma sak med dem. Men det kommer dröja flera veckor innan uppdateringen kommer.
- Alla verksamhetens filer är krypterade och det går inte att koppla upp sig på nätverket – även här kommer det ta lång tid innan det är åtgärdat.

Hur gick cyberattacken till?

Riksarkivet

En falsk e-post gick ut till alla i personalen …

Årets julklapp är en chokladask!

Klicka på länken och välj vilken du vill ha:

- Blandade sorter
- Vegan
- Sockerfritt
- Mörk choklad
- Lakrits

Obs! Sista beställningsdatum är den 6 december.

Cyberattacken berodde på att personal lurades av ett falskt e-post-meddelande och klickade på en länk. Resultatet var att skadlig kod laddades ned till deras datorer.

Hur många klickade på länken?

Svar:
154 personer

Riksarkivet

Vad säger personalen om cyberattacken?

- ”Jag har ett viktigt möte som jag inte kan ställa in!”
- ”Kommer det inte gå att göra någon lönekörning? Får vi ingen lön?”
- ”Har någon stulit information? Tänk om den handlar om mig?”
- ”Vad hände med alla filer jag hade sparat på datorn? De måste väl gå att återställa? Och fotografierna på mobilen?”
- ”Tänk om min privata dator har blivit smittad! Jag hade filer på USB för att kunna jobba hemma.”
- ”Kan vi inte bara betala lösensumman?! Jag måste kunna jobba!”

Cyberattacker skapar stress och oro hos de som drabbas.
Att ta hand om det är en viktig del av krishanteringen.

Riksarkivet

Hur lång tid tar det innan vi kan börja arbeta normalt igen?

Svaret är 48 dagar

Vad gör vi under den tiden?

Workshop: hur hanterar vi krisen?

Dag 1

Ännu vet ingen hur allvarligt läget är. Problemen kommer väl vara lösta på ett par timmar?

Dag 2

Nu vet vi att det är en allvarlig cyberattack och att telefoner och datorer är smittade. Vi börjar inse att det här kommer att ta tid – och vi är utlåsta från våra filer, IT-system, nätverk, digitala resurser …

Dag 3 till 48

Det står klart att krisen kommer bli långvarig. Räkna med flera veckor.

Krisövning: hur hanterar vi en cyberattack?

Det akuta skedet – när ingenting fungerar och information saknas om hur allvarliga och långvariga konsekvenserna av cyberattacken är.

- Vad får cyberattacken för omedelbara konsekvenser? (Exempelvis avbrott i pågående möten, arrangemang som kan behöva ställas in, ingen tillgänglighet till digitala resurser)
- Vem behöver få veta vad som händer och vad gör vi i det akuta skedet? Ska vi stänga ned verksamheten helt eller övergå till alternativa arbetssätt – vem beslutar om det?
- Hur kommunicerar vi internt och externt när det inte kan ske digitalt?

Krisövning: hur hanterar vi en cyberattack?

Alternativa arbetssätt

- Vilka arbetsuppgifter är möjliga att utföra? Vad *måste* vi göra?
- Hur påverkas externa om vår verksamhet inte fungerar? Hur ska vi kommunicera? Finns det alternativa lösningar för delar av verksamheten?
- Vad behöver din egen enhet för stöd från andra delar av verksamheten?
- Hur är resten av verksamheten beroende av din enhet?
- Finns någon utomstående som skulle kunna hjälpa till? Kanske en annan verksamhet som vi själva kan hjälpa om de drabbas?

Tänk på: vi är inte helt ensamma bara för att det här har hänt. Kriser hanterar vi tillsammans!

Riksarkivet

Krisövning: hur hanterar vi en cyberattack?

Utrustning och digitala verktyg

- Hur hanteras smittade telefoner och datorer? Ska de samlas in, lämnas till någon särskild ansvarig, eller vad gör vi?
- Hur hindrar vi att smittan sprids vidare? Vi vill ju inte att fler ska drabbas! Och vems ansvar är det om någon får sin privata mobil förstörd för att man försökte använda den istället för jobbmobilen?
- Identifiera behov av tillfälliga digitala lösningar, exempelvis för kommunikation externt och internt. Vad går att använda?

Tänk på: snabba lösningar kan göra krisen värre. Fundera över vad som går att förbereda så att det finns färdiga lösningar att ta fram om en kris inträffar.

Riksarkivet

Krisövning: hur hanterar vi en cyberattack?

Förberedelser och förebyggande åtgärder

- Vad kommer du att önska att ni inom din verksamhet hade gjort för att förbereda er?
- Vilka förebyggande åtgärder hade du velat att andra inom din egen verksamhet hade vidtagit?

- Vad gör ni själva på din avdelning eller enhet?
- Vilka förberedelser ska vara gemensamma eller samordnas inom hela organisationen?

Riksarkivet

Vad vet vi?
(regler för övningen)

Så sprids den skadliga koden:

1. Till datorer och mobiler via länkar i e-post
2. I det interna nätverket via delade mappar
3. Mellan datorer via USB-minnen och externa hårddiskar

- Datorer, mobiler och skrivare är nedlåsta.
- Nätverket och internet går inte att nå, varken trådat eller wifi.
- Alla digitala tjänster och webbplatsen ligger nere.
- Filer som sparats i nätverksmappar har blivit krypterade.
- Filer på USB, externa lagringsytor och bilagor i e-post riskerar att sprida koden vidare till andra.
- Filer som sparats lokalt på dator eller mobil går inte att rädda.

48

DAGAR

Diskutera i grupper

När vi är klara återsamlas vi för presentation och gemensam diskussion.

Att diskutera:

- Hantera det akuta skedet
- Alternativa arbetssätt
- Begränsa spridningen och hitta tillfälliga digitala lösningar
- Förberedelser och förebyggande åtgärder

Riksarkivet