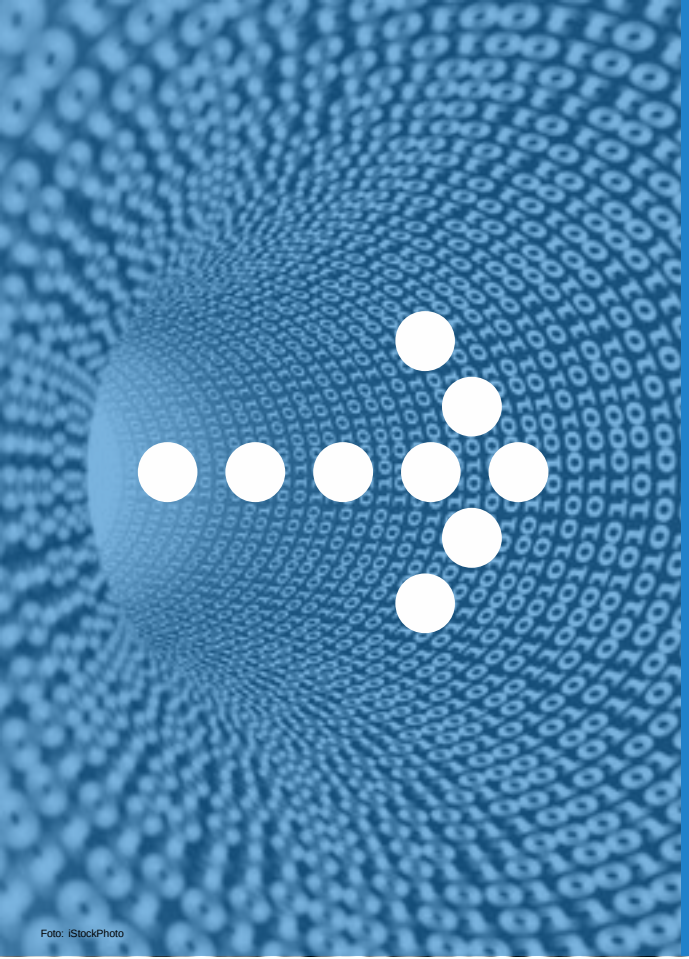


Foto: iStockPhoto

Pass 3
Incidenthantering i praktiken

Praktisk incidenthantering i industriella informations- och styrsystem

Myndigheten för samhällsskydd och beredskap

NCS3

FOI

NotPetya (Maersk)

- Vad hände
  - Malware spred sig och krypterade hårddiskar
  - Den globala IT-miljön slogs ut inom loppet av timmar.
  - Gisslanprogram?

Susan Maersk en route at sea. Källa: A.P. Moller, Maersk

NotPetya (Maersk)

- Konsekvenser
  - 49000 laptops utslagna ~100%
  - 3500/6200 servrar utslagna
  - All fast telefoni utslagen
  - Alla kontakter raderade från mobiler
  - DHCP-infrastruktur förstörd
  - 5% av global trafik störd
  - Kostnad: ca 2,4 miljarder kronor

Susan Maersk en route at sea. Källa: A.P. Moller, Maersk

NotPetya (Maersk)

- Förberedelse
  – ”…the recovery plans didn’t account for the global destruction of everything — a common line of thought in asset-centric businesses”.
- Upptäckt
  – Datorer stängdes av
- Hantering
  – Skickade hem lokala IT-tekniker
  – Hämtade den enda fungerande domänkontrollanten från Afrika
  – Byggde nytt Windows 10

Susan Maersk en route at sea. Källa: A.P. Moller, Maersk

NotPetya (Maersk)

- Efterarbete
  - 3000 nya anställda
  - Alla anställda får cyberutbildning
  - Troligen mycket mer vi inte vet

Susan Maersk en route at sea. Källa: A.P. Moller, Maersk

Norsk Hydro

- Vad hände
  - Första intrång via epost från kund
  - Månader senare har angriparna kontroll över AD
  - Group policy används för att köra krypteringsbinärer
  - Utpressningsbrev placeras på maskinerna som angripits

Photo: Norsk Hydro

Norsk Hydro

- Konsekvenser
  - Avbrott i produktion under flera veckor
  - Bulkproduktion mindre påverkad
  - Kostnad: ca 750 miljoner kronor

Photo: Norsk Hydro

Norsk Hydro

- Förberedelse
  - Metod, team och mandat fanns
  - Verktyg saknades
  - Sårbara system
- Upptäckt
  - Angriparen utlöste gisslanprogram*
  - Spårades till initialt angrepp via e-post

Photo: Norsk Hydro

Norsk Hydro

- Hantering
  - Arbetade systematiskt
  - Tog hjälp
  - Öppen kommunikation
  - Vissa verktyg saknades
  - Kontinuitetsplanering fallerade i vissa fall
- Efterarbete
  - Oklart, många förfrågningar

Gisslanprogram

- Vad hände
  - En användare klickade på en bilaga i sin privata e-post
  - På en timme krypterades ca 140 000 filer lokalt på nätverket
- Konsekvenser
  - Oåtkomliga filer under 3-4 dagar
  - Kostnad för återställning och nertid

Gisslanprogram

- Förberedelse
  - Skyddsåtgärder
  - Incidenthanteringsrutiner
- Upptäckt
  - Av en annan användare
  - Begränsat behov av analys
- Hantering
  - Stäng av och isolera system
  - Informera användare och ledning

Gisslanprogram – Efterarbete

- Slutsatser
  - Väldigt svårt att undvika
  - Incidenthantering fungerade enligt plan
  - Vikten av säkerhetskopior offline
  - Diversifierad filåtkomst
- Justering av skyddsåtgärder
  - Detektionsmekanism
  - Instruktioner för hantering
- Justering av miljö
  - Justering av filnamnslängd
- Information till ledning och användare
  - Påminnelse att inte klicka

National Health Service

- Vad hände
  - Gisslanprogrammet Wannacry sprider sig via SMB och infekterar 230 000+ maskiner.
  - I Storbritannien stängde programmet ner datorsystemen för 34 NHS-mottagningar varav 24 var akutmottagningar, plus 595 allmänläkarmottagningar

National Health Service

- Konsekvenser
  - Ett stort antal sjukhus kunde inte nå journalsystem eller använda epost.
  - Minst tre sjukhus fick stänga ner mottagningen för alla nya fall, inklusive akutfall.
  - Många läkarmottagningar kunde inte processa patienter
  - Fler än sex tusen patienter fick tider för behandling flyttade

National Health Service

- Förberedelse
  - Lokala myndigheter var ansvariga för infosäk.
    - NHS hade testat 88/236 verksamheter innan incidenten. Ingen klarade testerna.
  - Datorsystem ej uppdaterade, i många fall (5%) kördes fortfarande Windows XP
  - ”Hade brandväggar uppdaterats mot SMB-sårbarheten hade de varit skyddade”

National Health Service

- Upptäckt
  - När tjänster upphörde att fungera
- Hantering
  - Protokoll för katastrofer EPRR
    - Ej förberett för cyberscenarion
  - Stänga ner IT-system, försök t ö-drift
  - Incident-teams organiserades och sändes ut till sjukhus

National Health Service

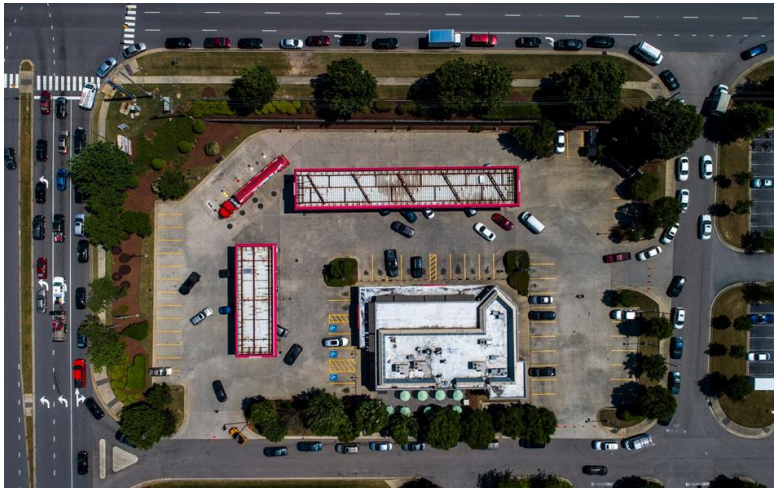
- Efterarbete
  - Upp till 20 000 patientbesök måste flyttas och senareläggas
  - En tidigare utvecklad plan för att hantera cyberangrepp kommunicerades ut och började testas.
  - Krav på utfasning av windows XP,
    - 1,4 miljoner 2017, 2000 kvar 2020

Colonial Pipeline 2021

- Vad hände
  - 29 april loggar angripare in på Colonials datornät via fjärranslutning
  - 7 maj,
    - 0500 datastöld, gisslanprogram och lösenbegäran
    - 0610 Pipeline stängs ner helt.
    - Mandiant kallas in
  - 8 maj, Colonial betalar lösen.

Colonial Pipeline

- Konsekvenser
  - Kontorssystem krypteras och företaget kan inte längre processa betalningar
  - Kunderna till Continental kan inte längre få bensin
  - Panik uppstår hos allmänheten som panikköper bensin.
  - Flera olyckor inträffar när bilar lastade med bensin fattar eld.



Colonial Pipeline

- Förberedelse
  - Ingen CISO, Cyberincidentplan eller –team
  - Öppna fileshares och fjärradminportar
  - Glömt VPN-konto, utan 2FA, kvar när profilen skulle ha stängts
  - *"…in this case, obviously it was the concern that we really had no vision into our IT or OT systems to understand the degree of corruption, and encryption, and it really took us days even with the help of world class expert [sic] by Mandiant to get there, so again, that's why that decision was made…"*

Colonial Pipeline

- Upptäckt
  - Inte förrän angriparna lade in lösenbegäran, efter att krypteringen redan aktiverats.
  - Angriparna hade sju dagars aktiv närvaro i näten.

Colonial Pipeline

- Hantering
  - Omedelbar nedstängning för att skydda sin pipeline.
    - Men gjord innan man visste om den var hotad eller ej.
    - Vet ej om den var hotad.
  - Tog in hjälp från Mandian omedelbart
  - Betalade lösensumma för att få upp systemen.
    - Okänt hur mycket data som återskapades

Colonial Pipeline

- Efterarbete
  - Med hjäp av Mandian återskapade man näten och upptog driften.
  - Trots lösenkoder varade stoppet en vecka.
  - Vittnade för kongressen om incidenten och varför de betalat.
  - DHS och flera andra federala myndigheter har inlett samarbete för att säkra upp rörledningen i framtiden. Inte mycket har framkommit i media

Extra mini-händelse

- Fel i vapnet upptäcktes december 2020 och offer kontaktades av de som hittat det.
- I januari 2021 hittade Bitdefender hålet och publicerade det. DarkSide tackade dem för informationen och fixade problemet.

Nyttja incidenter för lärande

- Kan samma motiv ge upphov till ett angrepp mot era system?
- Hur hade händelsen påverkar er miljö?
- Hur hade ni upptäckt händelsen?
- Har ni rätt skyddsåtgärder?
- Hur skulle ni ha hanterat händelsen?