VestfoldLAB AS

DATAINNBRUDD

VestfoldLAB AS

- Akkreditert laboratorium lokalisert utenfor Tønsberg
- Offisielt laboratorium for Mattilsynet
- Vinner av Mangfoldsprisen 2021
- Dannet 1962 som Kjøttkontrollen
- 15 fast ansatte
  - 2 i arbeidspraksis
  - 1 lærling
- Cirka 120 000 analyser årlig

Hvordan kunne det skje?

- Vi har, i følge IT, opp til 1 000 dataangrep i uken

Hvordan kunne det skje?

- Etter et strømbrudd 6/12 gjorde vi en rutinemessig kontroll at brannmuren, og fant ut at Geo databasen var skadet. Oppdatering/reinstallering av denne syntes vanskelig pga plassmangel på boksen, og ny router ble derfor bestilt.

Hvordan kunne det skje?

- Vi var kjent med at et sikkerhetshull i MS Exchange Server sammen med Windows server 2016 kunne utgjøre en risiko, og har hele tiden hatt Geo-blokkering i brannmuren slik at all trafikk til og fra Russland, Kina og Ukraina (bl.a.) har blitt stoppet. Siden Geo-databasen var nede, økte altså hackermuligheten betydelig.

Hvordan kunne det skje?

- Dessverre rakk hackerne å komme inn til oss før ny router var på plass. Alle maskiner i domenenettverket, med unntak av en, inkludert servere og backup NAS, var infisert. Maskinene med XP syntes å være forsøkt hacket, men disse var ikke kryptert. Dette kan tyde på at MS Bitlocker er benyttet i angrepet.

Øyeblikkelige tiltak

- XP-maskiner og andre maskiner tilknyttet analysemaskiner var derfor ikke effektivt angrepet, noe som gjorde saken litt enklere. Det ble etablert et isolert subnett der disse maskinene ble satt, der det ikke var tilgang på internett, hverken ut eller inn.

Øyeblikkelige tiltak

- Øvrige maskinvare ble formatert og OS ble reinstallert. Det forelå backup på flere nivåer og flere plasseringer, deriblant ekstern (Databackup Norge AS). Sistnevnte ble benyttet for restore, da det var enklere å finne igjen mest data der.

Øyeblikkelige tiltak

- En ny, ren maskin (nyinstallert OS, scannet med ByteWize og MS) ble koblet til internett, databackup ble installert, og databasen til laboratoriesysemet, samt dokumentarkiv ble tilbakeført.

Øyeblikkelige tiltak

- Siste backup var fra fredag 8/12, så vi mistet den siste ukens arbeid, samt at vi har oppdaget at det er bruddstykker fra tidligere, som vi mangler, av ukjente årsaker. Den rene maskinen ble også benyttet som midlertidig server til ny server var opprettet, og dataene kunne kopieres over til denne. Det ble satt opp en ren klientmaskin for å kjøre laboratoriesystemet, deretter ble maskiner lagt til etter hvert som de ble renset

Bakgrunn

- I følge IT har vi i perioder over 1 000 dataangrep i uken
- De kommer hovedsakelig fra Kina og Russland, og vi hadde merket et veldig oppsving fra Russland etter at krigen i Ukraina brøt ut
- Som et resultat av dette har vi Geo blokkering på alle IP-adresser utenfra Vest-Europa
- Vi har noen eldre maskiner, på kjemi, som trenger gammel programvare for å kjøre, disse gjorde oss ekstra utsatte

Aksjoner

- Vi varslet Norsk Akkreditering
- NA kom på oppfølgingsbesøk for å se hvordan vi hadde løst saken, hvordan systemene fungerte og får å sjekke at vi hadde fulgt rutinene og at vi hadde arbeidet etter NS-EN ISO 17025
- Vi gjennomførte prosedyrene tiltak ved driftsstans, risikoanalyse ble foretatt
- Tiltaksplaner ble iverksatt
- Avviksrapport ble utarbeidet

Hvordan ungikk en maskin angrepet?

En maskin kom uskadet fra angrepet. Den blir koblet ut av nettverket hver dag. Det var dermed den eneste maskinen hvor all e-post historikk fortsatt var intakt.

Hva kan vi lære?

Som så ofte så ble ikke problemet knyttet til strømbruddet og Geo databasen kommunisert videre forbi IT

Geo blokkering er kritisk viktig

Back-up oppdatering daglig

Hva «reddet» oss?

- Gode rutiner knyttet til driftsstans
- Data back-up av katalogsystemet vårt
- Data back-up av laboratoriesystemet vårt (siste backp var 6 dager gammel)

Hva reddet oss?

VestfoldLAB AS
RÅDGIVNING – MAT – KJEMISK ANALYSE – MIKROBIOLOGISK ANALYSE

Dokument ID	Versjonsnummer	Side 1 av 1
05	0.1	
Ansvarlig utgiver: Bent Mathisen		

P11A01S04 **Arbeidsskjema ved datasvikt**

Godkjent av: Roy Markussen **Status: Publisert**

Leverandør:		Tlf:
Prøvedato:	Prøvetaker initialer:	Prøvehenting stk. Prøvetaking stk. Prøvetaking+henting stk.

Renholdskontroll □ Hygienisk kvalitet □ Matforgiftning □ Bassengvanns prøve □ Kimtallsprøve □
Kjemi □ Beh. vann hoved p. □ Beh. vann tappe p. □ Ubeh. vann tab. 6.1 □ Legionella □

Merknader

Analyseparameter		Fortynning avlest		Verifisering		Resultat	Dato	Sign.

Registrert/Besvart: /	Analyserapport:	Sign:

Hvordan vi jobbet

1. Vi tok frem våre prosedyrer
2. Satt i gang nødprotokoll (Tiltak ved driftsstans)
3. Vi laget og tok i bruk midlertidig prosedyre for avviksbehandling
4. Tok i bruk midlertidig prosedyre for dokumentstyring
5. Utarbeidet risikoanalyse knyttet til dataangrepet
6. I og med at kvalitetssystemet vårt brøt sammen laget vi en list over åpne avvik

Tiltaksplaner

1. Skifte passord i hele organisasjonen
2. Kontakte kunder og forklare situasjonen
3. Flytte e-post (office365) i skyen, 14. desember
4. Installere ny router
5. Installerte ny Windows server
6. Starte nedlasting fra online back-up
7. Få laboratoriesystemet operasjonelt
8. Sette opp nettsiden igjen slik at vi kan informere også på den måten
9. Få opp systemet for å sende ut prøveresultater
10. Innhente og installere nytt kvalitetssystem
11. Sikre normaldrift ASAP
12. Starte prosessen med innkjøring av nytt skybasert laboratoriesystem