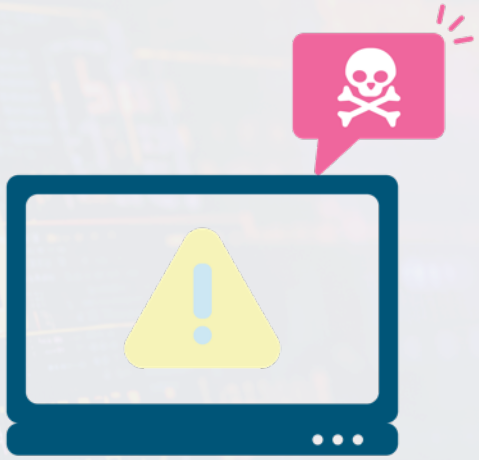
TECHTRADE

WEBINAR

Nya typen av IT-attacker mot sjukvården

CARLANDERSKA

Kraftig ökning av anmälda dataintrång



Vad gör TechTrade?

- Vi ska bidra till ett friskare samhälle genom att kunderna får mer patienttid
- Strategiska samarbeten
- Delad kunskap (1+1=3)
- IT avdelning till +200 privata vårdenheter runt om i Sverige
- IT inom vården i fokus sedan 1993

Carlanderska – Möjligheternas sjukhus

- **Wictor Bennet Winsnes**, IT-chef på Carlanderska sjukhuset

CARLANDERSKA

TECHTRADE

CARLANDERSKA

Sammanställning av IT-incident 2023-11-27

CARLANDERSKA

Kort om Carlanderska

Bolagsform	Stiftelse
Anställda	370
Verksamhet	Operation, Vårdavdelning, Röntgen, Vårdcentral mm.
Partners	12 Vårdpartners

IT	
IT-avd.	6 personer (2 tekniker, 3 IT-admin + chef)
IT-stöd	Konsultfirma 4h / vecka
IT-Säk	Fortigate, Symantec mm
Miljö	320 klienter, 45 servrar, 30 switchar

Incidenten..

03:30	Larm	Backup förlängd körtid - Ingen åtgärd, normalt
06:30	Larm	System otillgängligt - Felsökning av tekniker påbörjas
06:40	Samtal	System otillgängligt - Eskalering av ärende - LG informeras
07:00	IT	Konstaterar intrång - Krisplan (IT) initieras
08:30	Först.	Förstärkning IT konsulter anländer

IT-Krisledning

Nivå 1	Grön	Daglig drift
Nivå 2	Gul	Störning
Nivå 3	Orange	Stabsläge
Nivå 4	Röd	Förstärkt stabsläge

Nivå III

-Allvarlig påverkan på verksamheten, vissa system otillgängliga
-Drift osäker
-Omfattning Stor
-Ev. patientpåverkan
-Ledningsgruppen meddelas, Krisgrupp sammankallas

Åtgärder
Samtlig personal på IT-Avdelningen informeras och tilldelas uppgift (enl. förutbestämd matris, tex, kontaktperson, Ledningsansvarig, IT-Resurs kallas in.

Bedömning av omfattning, Segmentering, Nedstängning mm.

CARLANDERSKA

Stabsläge – Krisgrupp LG

06:42 Samtliga i Ledningsgruppen informeras via ”VML-funktionen”
”Akut driftstörning IT, påverkar alla system, felsökning pågår”
(Manuella rutiner förbereds och tas i bruk)

07:02 Omfattning / påverkan för verksamheter meddelas
Varje enhet meddelar vem som är kontaktperson

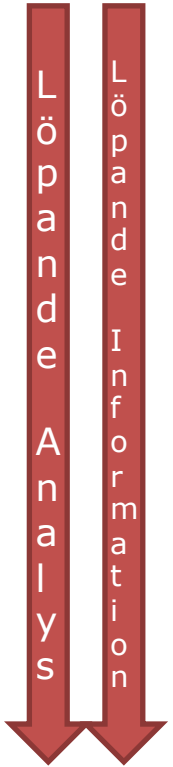
07:53 Sjukhuschef meddelar Stabsläge och meddelar möte 08:05

08:05 Stab (LG) Samlad

Verksamheter, Påverkan

Vårdcentral	Gul	Vissa datorer påverkade, Vissa kopplingar
Vårdavdelning	Gul	Vissa datorer påverkade, Vissa kopplingar
Kir/ort	Gul	Vissa datorer påverkade, Vissa kopplingar
Operation	Orange	System nere, vissa datorer påverkade
Röntgen	Orange/Röd	System nere, vissa datorer påverkade
Admin	Orange	System nere, vissa datorer påverkade
Partners	Gul	Åtkomst till CS spärrat (av säkerhetsskäl)

Fas	Åtgärd
Omfattningsbedömning	Vad är drabbat, hur mycket är drabbat Server, klient Påverkan på system
Påverkansbedömning	**Vilken påverkan på verksamheten** Hela sjukhuset Nivå 3 (orange) Dock kan flera verksamheter fortlöpa med manuella rutiner, dock med begränsad prestanda
Uppsäkring	Eliminera/Minimera fortsatt skada Bedömning att strypa förbindelser såsom VPN, utökade nät mm
Åtgärd	Vilka åtgärder vidtas för att upprätta funktion Uppsättning av ny miljö efter det att vi kan ”garantera” säker drift.



Krishantering IT

Interna resurser

IT-chef	Ansvarar för kommunikation till LG (krisgrupp)
IT	Ansvarar för samordning av resurser, kommunikation på enheten, dialog med konsultfirma (Insatsteam)
IT	Genomlysning av loggar (brandvägg, server, klient mm)
IT	Uppsättning av skyddad ny miljö
IT	Uppgifter / Uppsättning av skyddad ny miljö
IT	Uppgifter / Uppsättning av skyddad ny miljö

Externa resurser (konsultfirma)

Konsult	Teamleader / Tekniker Primär kontakt för Carlanderska
Konsult	Insatspersonal / Tekniker Kontakt med Leverantör av Brandvägg (Fortinet) , System (VM-ware, Symantec mm)
Konsult	Insatspersonal / Tekniker Distrubrition av system som kan ”avlusa”
Konsult	Insatspersonal / Tekniker

BitLocker recovery

Enter the recovery key for this drive

Use the number keys or function keys F1-F10 (use F10 for 0).
Recovery key ID (to identify your key): 4290B6C0-B17A-497A-8552-272CC30E80D4

Here's how to find your key:
- Contact your organization's help desk
- For more information go to: aka.ms/recoverykeyfaq

CARLANDERSKA

Viruset / Personerna bakom

Drabbat?
- Microsoft Windows-servrar (samtliga versioner)
- 40 % av alla klienter (ca 100 st)

Bitlocker låsta, med en modifierad version Bitlocker

Vi bedömer inte i dagsläget att man har kunnat ta data, utan ”endast” ha låst vår miljö.

Viruset benäget att förändra sig, bygger på AI, som anpassar sig till ”Kundens” miljö

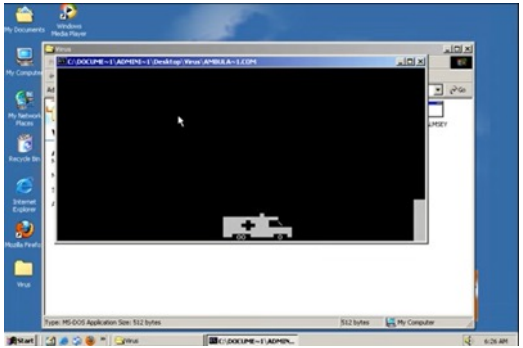
Syfte:
10 Miljoner SEK i Bitcoin

Bitcoinkursen…

Följer ruskigt likt grafen för ransomware attacker

Viruset / Personerna bakom

Vilka är de?



80,90,00-talet

Vem : 15-30 år Dataintresserade oorganiserade, eller mindre grupp

Syfte : Göra sig ett namn

2020->

Vem : Stat/Företag, Bolagsstruktur, Chefer teamleaders, tekniker mm

Syfte : Desinformation, skapa instabilitet, vinstintresse, terror

CARLANDERSKA

Slutsatser

Slutsats efter daglig dialog

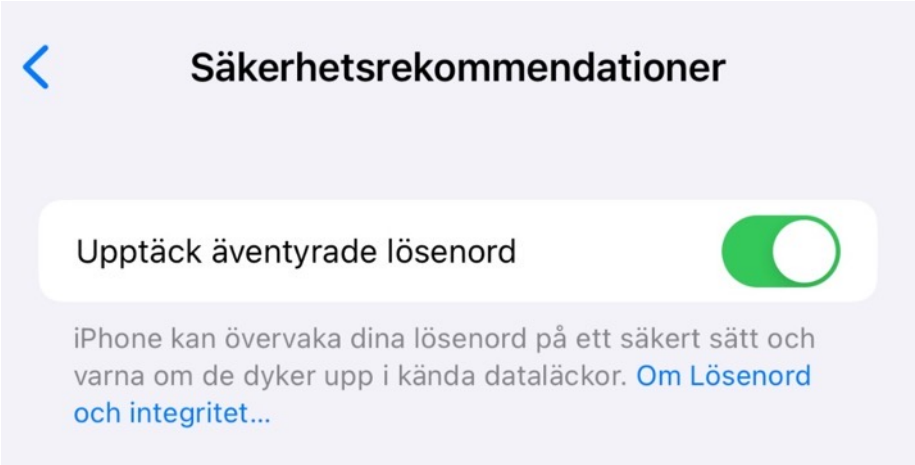
Om Hackergruppen
- Stödjer Ryssland
- Erbjuder 24/7h support
- Garanterar en säker IT miljö
- Investerar i BitCoin
- Infiltrerar Firmware (hårdvarunivå)
- Infiltrering (tunnel) görs månader innan (och säljs på DarkNet)

*

Visa användare på tex APT möte (Iphone)

Tänk på
- Immutable backup samt ”tvätta backupen”
- Stark autentisering (SITHS mm)
- Glöm inte hårdvarupatch
- Segmentera VLAN (separera kaffemaskinerna,fastighet)
- Utbilda personal*, penetrationstesta

Iphone / inställningar / Lösenord →



CARLANDERSKA

Frågor?

PANELDISKUSSION

Wictor Bennet Winsnes

CIO/CTO på Carlanderska sjukhuset

Jan Lindblad

VD och grundare av TechTrade

Johnie Berntsson

CIO/CTO på TechTrade

TECHTRADE


TECH
TRADE
CREATES TIME
Ha en trevlig och trygg dag!