Cyberhot

OCH VAD VI KAN GÖRA ÅT DEM

Stockholm 2024-11-28

SÄKERHETSLÖSNINGAR FÖR FÖRETAG

01 Säkerhetssimuleringar och träning

02 Riskbedömningar och säkerhetsrådgivning

03 Säkerhetsmedvetenhet och utbildning

04 Realtidsövervakning och respons

05 Pentestning och sårbarhetsanalyser

06 Kontinuitetsplanering och verksamhetsåterställning

07 Strategisk säkerhetsoptimering

08 Sidia Pass – Lösenordslös autentisering

09 Sidia Inspector – Sårbarhetsskanning för Microsoft 365

BiTA

SIDIATECH

BiTA Service Management

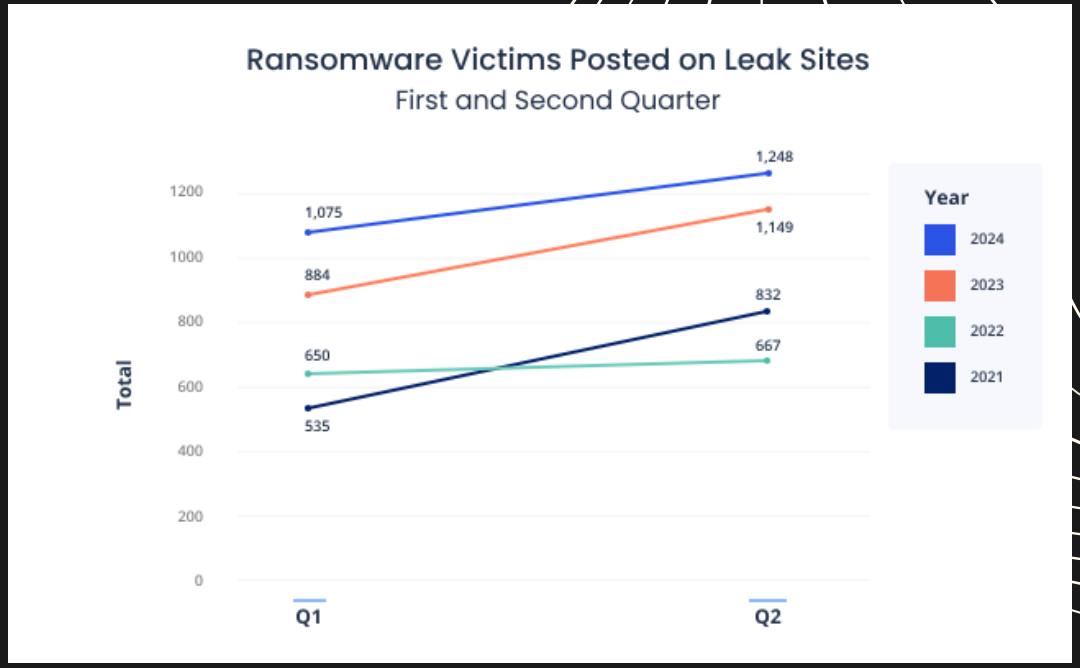
ETT KUNSKAPSFÖRETAG SOM ERBJUDER IT-DRIVEN VERKSAMHETSUTVECKLING TILL ORGANISATIONER SOM VILL SKAPA INTERN EFFEKTIVITET OCH KUNDNYTTA

- **Cirka 15 anställda och 5 associerade** förändringskonsulter som arbetar i uppdrag som består av **utbildning** och **konsultation.**
- BiTA grundandes 2003 och är verksamma i hela landet.
- **Våra kompetensområden:**
  - ITSM
  - Governance och Compliance
- **Våra leveransformer**
  - Konsultation
  - Utbildning

supportservices institute - en del av BiTA

VARFÖR SKYDD MOT RANSOMWARE ÄR AVGÖRANDE

I juli 2024 krävde och mottog Dark Angels-gänget en rekordstor lösensumma på 75 miljoner dollar från ett företag i en ransomware-attack. Detta markerar en av de största betalningarna någonsin och visar hur cyberbrott och ransomware-attacker blir alltmer sofistikerade och kostsamma, med enorma konsekvenser för företag världen över.



SIDIATECH

Att förebygga

BiTA

- Ledningens ansvar
  - Tid och resurser
- Omvärldsbevakning
- Utbildning och informationsspridning
- Arbeta riskbaserat – utgå från en riskanalys

SÅ SKYDDAR DU MOT RANSOMWARE

SÄKERHETSKOPIERING

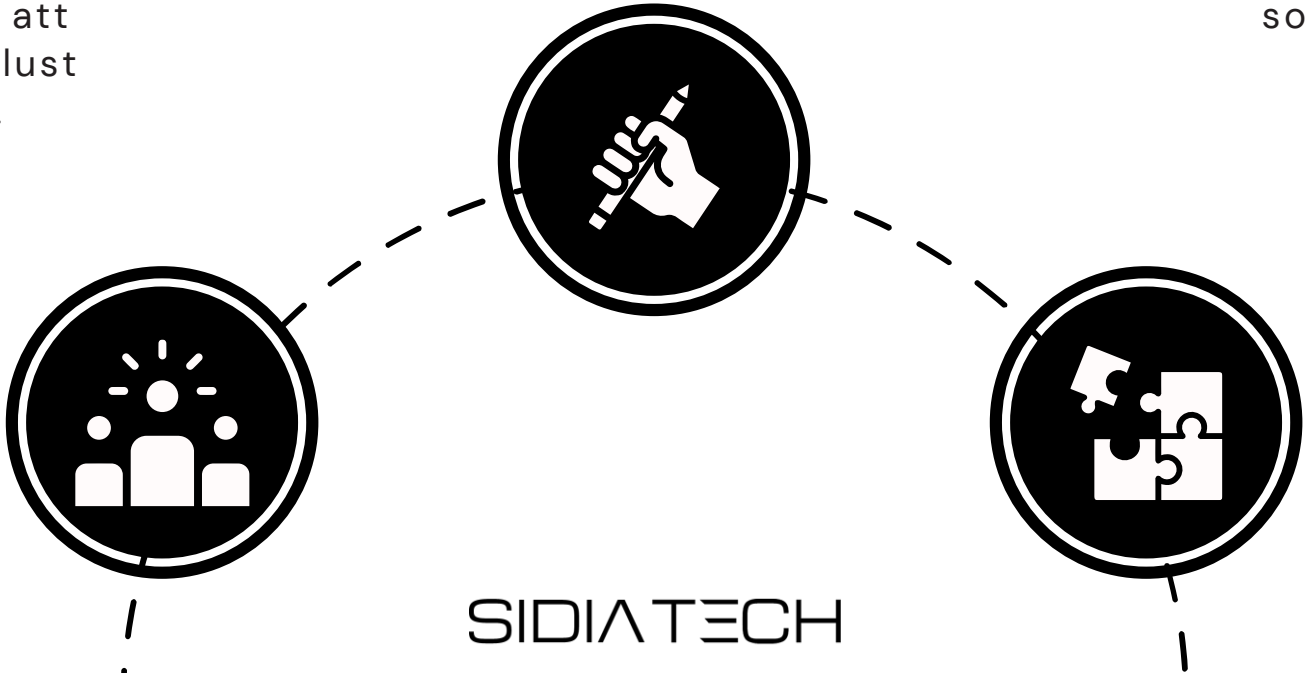
Säkerställ att alla viktiga data regelbundet säkerhetskopieras och lagras offline för att förhindra dataförlust vid en attack.

MEDARBETARUTBILDNING

Utbilda anställda om riskerna med phishing och hur man känner igen skadliga länkar och bilagor.

SYSTEMUPPDATERINGAR

Håll system och programvara uppdaterade för att eliminera sårbarheter som ransomware kan utnyttja.



SIDIATECH

Att upptäcka

BiTA

- All utbildning ska bära frukt
  - Inte klicka på länkar
  - Tänk på vad du säger och vem du håller upp dörren för
- Rutiner och kontaktvägar klarlagda, dokumenterade och välkända
- Incident management uppdaterad med säkerhetsrutiner

SÅ UPPTÄCKER DU RANSOMWARE

Att upptäcka ransomware tidigt är avgörande för att minska skadorna och snabbt kunna reagera.

Använd avancerade övervakningsverktyg som snabbt kan identifiera misstänkt aktivitet och varna vid potentiella hot.

HOTÖVERVAKNING I REALTID

Implementera system för att upptäcka ovanliga beteenden i nätverket, såsom plötsliga dataöverföringar eller oväntade åtkomstförsök.

ANOMALIDETEKTERING

Uppmuntra anställda att omedelbart rapportera misstänkta e-postmeddelanden eller ovanliga aktiviteter.

MEDARBETARENS RAPPORTERING

BiTA

SIDIATECH

Att hantera

BiTA

- Kan mycket väl utnyttja Major incident rutin – om den finns
- Det är viktigt att inte nöja sig med dokumenterade rutiner
  - Öva – utvärdera – öva igen
- Kommunikationsplan
- Viktigt att gå till botten med incidenten
  - Hur kunde det ske?
  - Vad ska vi göra för att det inte skall ske igen
  - Vad gjorde vi bra? Mindre bra?
- Rapportering

SÅ HANTERAR DU RANSOMWARE-ATTACKER

INCIDENTHANTERING: Ha en tydlig plan för att snabbt isolera och hantera incidenten samt minimera påverkan.

KOMMUNIKATION OCH UTVÄRDERING: Informera anställda och intressenter om situationen, och genomför en efteranalys för att stärka framtida skydd.

BiTA

SIDIATECH

Att återskapa

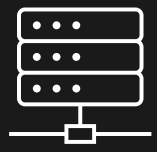
BiTA

- Två delar i detta arbete. Vi ska ha planer för:
  - Kontinuitet – verksamheten
  - Återskapande – IT
  - Consensus
- Planer inom båda områdena
- Konsekvensanalys (BIA) enligt SS-EN 22301:2019
- Ändringshantering skall kontrollera om återskapandeplaner påverkas!

ÅTERHÄMTNING EFTER EN RANSOMWARE-ATTACK

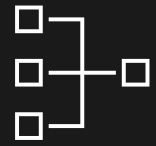
Ha en plan för att kritiska funktioner kan fortsätta även under återhämtningen.

KONTINUITETSPLANERING



Återställ data från säkra säkerhetskopior för att minimera dataförlust.

DATAÅTERSTÄLLNING



Utför en genomgång av alla system för att säkerställa att skadlig kod är helt borttagen innan drift återupptas.

SYSTEMGRANSKNING

BiTA

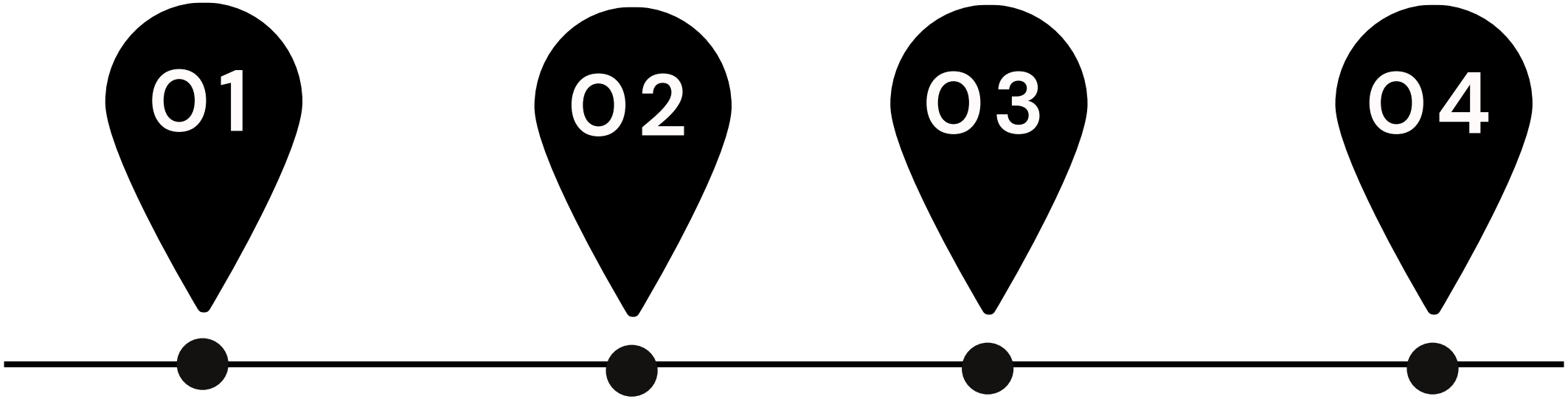
SIDIATECH

Att ständigt förbättra

BiTA

- Vi får inte enbart tänka ”operativt” utan måste ge oss tid för reflektion och förbättringar
- Skall vara någons ansvar!

UTVÄRDERA OCH FÖRBÄTTRA SÄKERHETEN



REGELBUNDNA SÄKERHETSGRANSKNINGAR

Identifiera nya sårbarheter och se till att skyddsåtgärderna är uppdaterade.

INCIDENTANALYS OCH LÄRDOMAR

Analysera tidigare incidenter för att stärka försvar och strategier.

UPPDATERADE SÄKERHETSPOLICYER

Anpassa och förbättra säkerhetspolicyer i takt med förändrade hotbilder.

LÖPANDE MEDARBETARUTBILDNING

Se till att personalen hålls uppdaterad om de senaste säkerhetsrutinerna och hoten.

BiTA

SIDIATECH

Kalix kommun

VAD HÄNDE

- Straxt innan 03.00 upptäcker hemtjänsten att något är fel
- Tack och lov har hemtjänsten alternativa arbetssätt och är förberedda på att använda sig av papper och penna
- Vid pass klockan 07 förstår man att ”ingenting fungerar”
- All data på alla system på alla datorer och på alla servrar slogs ut i hela kommunen
- Det står klart att det är en ransomwareattack där man krävde en lösensumma
  - ”Aldrig att vi betalar!”

Tro nu inte att det bara drabbar Kalix kommun...

Litet Axplock

DESSA HAR MEDGETT ATT DE BLIVIT DRABBADE

Tieto

COOP

Svenska kyrkan

Lunds universitet

Bauhaus

Frågor?

Tack för oss!

Anders Brunberg
Mail: anders.brunberg@bita.eu
Tel: 070-570 7672
www.bita.eu

Kerim Sidia
Mail: info@sidiatech.com
Tel: 08-502 437 82
www.sidiatech.com