nixu
cybersecurity.

Game Over eller kan vi göra något?

magnus.vallstedt@nixu.com

2019-10-23

Game over eller kan vi göra något?

Agenda

- Introduktion och diskussion om problemställningen
- Checklistor och Standards
- Summering och Go Do's

nixu

Introduktion

- Vem är Magnus och varför ska ni lyssna på honom?
- Utbildad i Informationssäkerhet i mitten-slutet av 80-talet och har sedan dess jobbat med informations- och IT-säkerhetslösningar inom bolag, banker samt myndigheter upp till Försvarssekretess
- IT-Konsult sedan 1989 och leder nu en Cybersäkerhetsarkitektgrupp på Nixu AB
- Har under åren tagit fram ett antal olika Blueprints/Guidelines för att förenkla och höja Informations- och IT-säkerheten på ett strukturerat sätt inklusive säkrad cybersäkerhetsarkitektur inom ovanstående brancher

Trusted go-to partner for cybersecurity services

Vision:
Keeping the digital society running

Mission:
Be the best workplace for cybersecurity specialists

approx
400+
Cybersecurity specialists

11 **Locations:**
Finland, Sweden, Netherland, US, Denmark Romania and Australia and more

Cybersecurity services from board decisions to deep forensic investigations

Founded in:
1988
publicly listed:
2014

98%
of our clients recommend Nixu

nixu
cybersecurity.

What could possibly go wrong?

Game over eller kan vi göra något?

Läget i Sverige hösten 2019

NÄRINGSLIV 21 oktober 2019 09:31

Ökad it-brottslighet mot företagare

Allt fler företagare utsätts för it-brott, visar en ny undersökning. Konsekvenserna kan vara förödande för verksamheten. Men det går att öka säkerheten med ganska enkla metoder, tipsar MSB:s expert.

TT

Andelen företagare som under de senaste två åren utsatts för it-brott har ökat från 19 till 29 procent sedan förra året, enligt en undersökning från Företagarna. En orsak är den ökade digitaliseringen.

– Man kanske hoppar på tåget för fort utan att förstå vad som kan hända, säger Carl Önne, informationssäkerhetsexpert på Myndigheten för samhällsskydd och beredskap (MSB).

Virus, dataintrång, id-kapning, stulna lösenord och utpressningsprogram är några av de brott som företagare riskerar att utsättas för. I många fall kan konsekvenserna för verksamheten vara förödande. Samtidigt ska man inte vara rädd för att digitalisera, anser Carl Önne.

https://vdtidningen.se/allt-vanligare-med-it-brott/

Game over eller kan vi göra något?

Filmtime:

- https://youtu.be/qbUh1U7lqjM

Diskussion om problemställningen

- Hur många finns i er organisation?
- Vad är det som är svårt?
- Vad behövs hjälp med?

Hur gå till väga för att säkra sej?

Finns det standards att använda som stöd i arbetet?

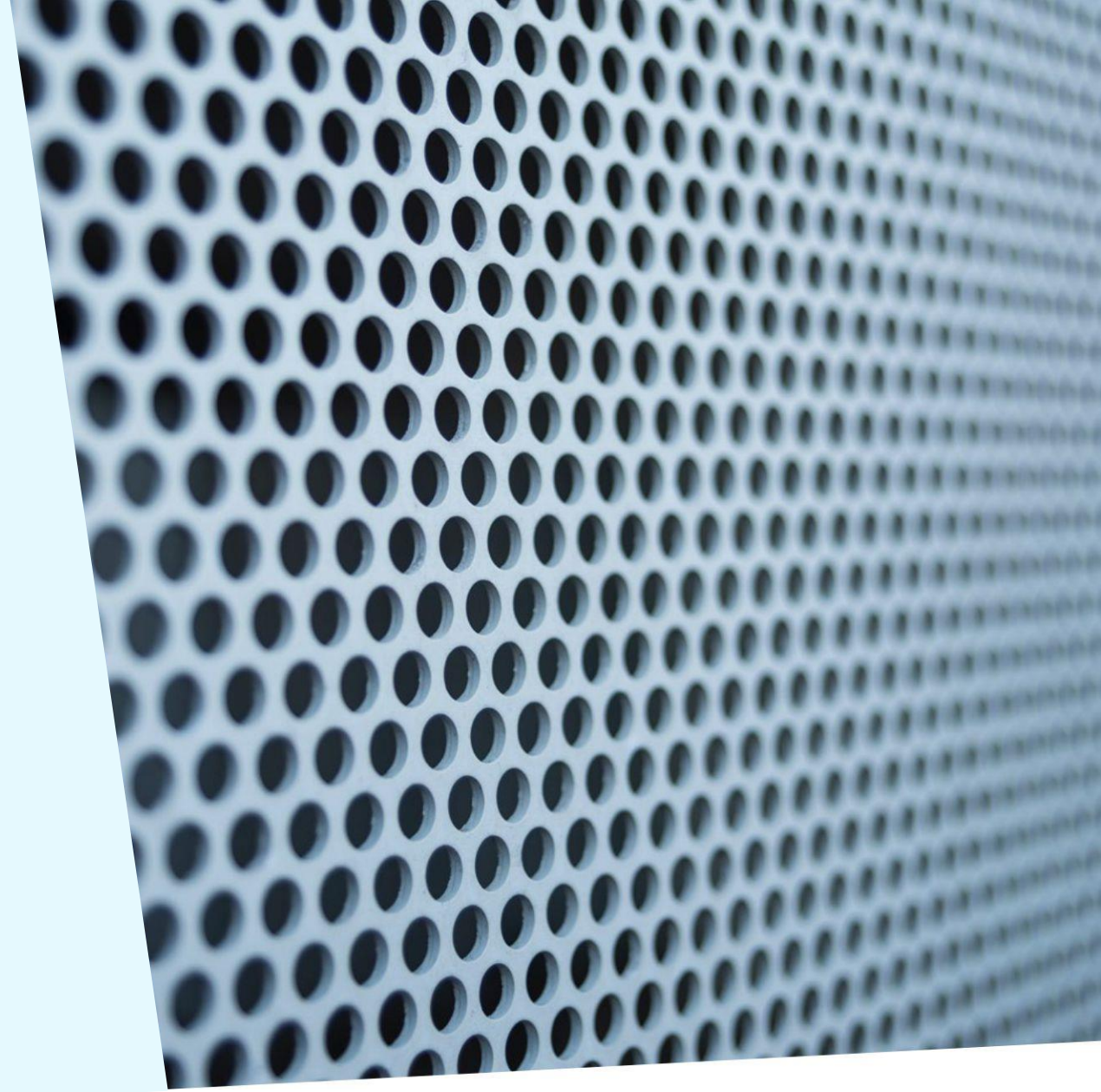
- Måste man uppfylla någon Informations och IT-säkerhetsstandard? Bra med standard med komplext på kort sikt.
  - GDPR
  - NIS
  - KSF 3.x eller senare
  - ISO2700x
  - CIS Top 20 Critical Controls
  - NIST CSF
  - DevSecOps
  - Penstests
  - Branschspecifik standard för att få sälja eller jobba med vissa lösningar ….

Checklistor – vad kan du göra snabbare och enklare?

Checklistorna är till för att förenkla ert arbete för att snabbt komma igång med prioriterade säkerhetshöjande åtgärder. Börja från lista nr 1 och jobba dej igenom punkterna.

- Vad ska jag/vi göra inom vårt bolag och vart ska vi börja?
- Hur sprider vi kunskap inom vår organisation om och varför vi behöver förändra vissa rutiner och tekniska lösning?
- Vad kan/ska vi kräva av våra leverantörer/partners/kunder?
- Hur kontrollerar jag att säkerheten fungerar som tänkt?

Checklistor att använda



Checklista 1 – Tänk säkert, Logga in säkert

- Prata internt om hur/varför ni ska skydda er information regelbundet. Stärk er säkerhetskultur!
- Vet ni vart er känsliga information finns som ni inte kan bli av med eller få förstört?
- Se till att alla anställda använder tvåfaktorsinloggning/2FA för all inloggning. Börja med Mail/Webmail, sedan Molntjänster (O365 etc)
- Se regelbundet över vilka tjänster, appar och inloggningar företaget använder. Oftast behöver inte alla på bolaget ha tillgång till all information och alla system. Glöm inte spärra access direkt när någon slutar!

Checklista 2 – Grunläggande datorhygien

- Ta backup regelbundet. Se till att backup görs på all information och eventuella konfigurationer för era appar/program/system
  - Har ni testat att återställa information från backuperna?
- Slå på automatisk uppdatering av allt. Antivirus, operativsystem och appar/programvaror mm på alla datorer, telefoner, plattor, servers, IoT
- Se till att bolagets alla datorer, telefoner, plattor och andra enheter har automatiskt skärmlås påslaget.
  - Slå på Biometrisk inloggning för att underlätta upplåsning
- Fundera på om ni ska ha separata datorer, telefoner, plattor för ert privata liv och arbetet med helt olika inloggning

Checklista 3 - Säkert nätverk på kontoret och på resande fot

- Köp VPN-App till alla era datorer, plattor och mobiltelefoner som automatiskt kopplar upp och säkrar er internetförbindelse över Wifi mm
- Skapa och använd konto på din dator som endast är vanlig användare och inte administratör på datorn
- Skydda nätverkets Router direkt när ni installerar den med ett helt nytt långt administrativt lösenord. Skriv ner och spara detta lösenord inlåst.
  - Slå på automatiska programvaru-/firmwareuppdateringar på all nätverksutrustning om möjligt. Annars kontrollera om det finns uppdatering var 90 dag, sätt tex remider i kallendern.
- Installera ett separat Wifi-Gästnätverk för besökare på kontoret med ett helt annat lösenord än ert interna nätverk. Där ansluter ni även IoT-enheter

Checklista 4 – Säker användare på kontoret och på resande fot forts.

- Lämna aldrig ut dina lösenord eller koder till någon annan. Oavsett!
- Om du måste använda lösenord istället för tvåfaktorinloggning/2FA så använd en lösenordsgenerator/lösenordshanterare
  - Generera alltid lösenord med en lösenordshanterare
  - Alltid unika lösenord per tjänst/system
  - Återanvänd aldrig lösen någonstans
  - Skriv gärna ner lösenorden på papper och lås in (bra när strömmen gått), eller använd en lösenordshanterare eller lösenordsåterställning och skapa nytt varje gång

Checklista 5 - Skydda dina (kort)uppgifter

- Tillåt aldrig websidor/webläsare eller appen att spara person- eller kortuppgifter (speciellt inte kort-/bankuppgifter)
- Använd bankens säkerhetslösning för att spärra dina bankkort för internetköp. Öppna kortet tillfälligt för köp online.
  - Slå på BankID-verifiering vid köp online (ex 3D-secure mfl), löser dock inte allt
  - Använd ett separat kort för köp online som inte är kopplat till ditt lönekonto
- Godkänn/Signera dina leveranser direkt i PostNords App mha Mobilt BankID så ingen kan utge sej för att vara du med falskt id
- Använd telefonApp för att skydda dina samtal. Tex Appen Signal på din Smartphone och se vem som ringer, messar, kör videosamtal med dej etc

Checklista 6 – Skydd dina smarta saker

- Välj bara leverantörer du känner till och litar på samt kontrollera att leverantören erbjuder löpande och automatiska uppdateringar
- Se till att slå på krypteringsskydd på dina Enheter/hårddiskarna/minnen.
  - Alla moderna telefoner, plattor, Windows- och Macdatorer etc har dessa funktioner inbyggt men du måste oftast slå på detta manuellt
- Överväg om du verkligen behöver koppla upp dina enheter respektive koppla bort de enheter du inte längre använder från Internet.
- Får din enhet inte längre uppdateringar från leverantören. Byt ut snarast.

Checklista 7 – Skydda dej och bolaget, ej teknik

- Skydd mot företagskapning – Skaffa digital brevlåda (ex Kivra) och ladda ner Bolagsverkets App så ser du vad som händer med bolaget
  - Få ett meddelande varje gång en anmälan om registrering kommer in, https://www.verksamt.se/minasidor
- Spärra dej från att utnyttjas som styrelsemålvakt i bolag. Anmäl dej gratis till https://bolagsverket.se/polopoly_fs/1.19046!/Menu/general/column-content/pdfFile/740.pdf
- Spärra din privatadress mot adressändring mha Adresslåset: https://www.adressandring.se/private/watch

Summering och Go Do's

Summering och Go Do's

- **Vänta inte!** Börja imorgon, boka av lite tid i kalendern varje vecka tills ni tagit er igenom dessa checklistor, börja från nummer 1 och arbeta dej igenom.
- Tänk på att alla förbättringar, även små, gör skillnad. Börja smått och öka
- Använd Checklistorna som stöd
- Tveka inte att ta hjälp av någon extern om ni inte kan eller hinner med själva eller hjälp att verifiera att ni lyckat med ert arbete att införa åtgärderna
- Ställ krav på att era egna leverantörer tar Informations- och IT-säkerhet på allvar. Kravställ i alla avtal och affärer att de följer en info-/itsäk-standard
- Använd ert Informations- och IT-säkerhetsarbete som en USP (Unique Selling Point) att ert bolag tar detta på allvar

Bra länkar

Aktivera 2-faktorauthenticering/2FA. Normalt gratis och finns för både privattjänster och företagstjänster

- AppleID: https://support.apple.com/en-us/HT204915
- Microsoft Office365: https://support.office.com/sv-se/article/konfigurera-tvåstegsverifiering-för-office-365-ace1d096-61e5-449b-a875-58eb3d74de14?ui=sv-SE&rs=sv-SE&ad=SE
- Google: https://www.google.com/landing/2step/
- LinkedIn: https://www.linkedin.com/help/linkedin/answer/531

Guider för att slå på 2FA för många olika tjänster på Internet

- https://twofactorauth.org/ https://authy.com/guides/

Bra länkar forts.

- Har du fått Ransomware? Här kan du få gratis hjälp att låsa upp många https://www.nomoreransom.org/sv/index.html

nixu
cybersecurity.

Follow us

nixuoy
@nixutigerteam
@nixuhq
company/nixu-oy

www.nixu.com