Effektivare säkerhetsarbete och processer = mycket mer än bara sårbarhetshantering!

- Gång på gång skrivs/berättas det om att en organisation råkat ut för
  - ransomware
    - Maersk
      - 1 st sårbarhet
        - USD 250 - 300 miljoner
  - förlust av persondata
    - BA
      - 2 % sanktionsavgift på globala omsättning
      - 2,3 miljarder kronor
  - intrång
    - personuppgiftsincident
      - Marriott
        - 1 st sårbarhet
          - 2 % sanktionsavgift på globala omsättning
          - 1,2 miljarder kronor
  - etc
- En viktig orsak, kanske den viktigaste
  - Många organisationer släpar efter med att förebygga och stänga sårbarheter
- Med tanke på att dataskyddsmyndigheterna beviljäger börjar ta betalt för personuppgiftsincidenter
  - Vad skulle en sanktionsavgift på 2% på omsättningen innebära för din/din organisation?
    - Egentligen
      - 2% eller 10 miljoner Euro
      - 4% eller 20 miljoner Euro
  - Vilken "försäkringsavgift" / Hur mycket är rimligt att avsätta/hålla för att förebygga denna risk?
    - Vad behöver ni göra?
    - Vad får ni för detta?
- Alla organisationer med någon form av it-verksamhet behöver hantera
  - Tillse att ledningen intresserar sig
  - Härdning / IT Security Baselines
  - Säkerhetsinformation/varningar från leverantörer Security Advisories
  - Resultat från sårbarhetsscanning
  - Resultat från penetrationstest
  - Hantering och uppföljning av "accepterade risker"
  - Patchning
  - Information, beslutsunderlag och "verktyg"
    - Ledning
      - KPI'er
        - övergripande
    - Mellanchefer
      - KPI'er för deras verksamhet
    - Utförare
      - anpassade "arbetsordrar" som verkligen underlättar deras jobb
- Dessa "pusselbitar" kan och bör i själva verket hanteras på samma sätt. Alltså inga stuprör utan ett samordnat arbetssätt/en samordnad process och rutiner
  - samt där så behövs, verktyg
    - Verktyg är inte nödvändigtvis detsamma som något it-system, det kan vara en kanbanboard, en pärm med instruktioner etc etc
- Kedja av åtgärder som behöver passa ihop
  - IT Security Baseline
    - Det behövs en baseline för ?mu?fins
      - Finns något som vi kan använda redan?
      - behöver vi bygga den själva?
    - Definiera baseline med utgångspunkt i
      - Organisationens styrande dokument
      - Standard
        - ISO 27002
        - ISF Good Practice
        - NIST
      - Best practice
      - Leverantörers
        - best practice
        - rekommendationer
      - Organisationens krav/behov/styrande dokument styr tekniken, Inte tvärtom!
      - Hämta inspiration t.ex. från sårbarhetsscanners
    - Baseline på remiss
      - Installera testsystem
      - justera i enlighet med synpunkter
      - ok - fortsätt med planering av implementation
    - Bestäm vilken nivå i organisationen som fattar detta beslut
    - Beslut - baseline ok
    - Uppdatera "installationsmedia" som används för nyinstallation
    - Planera införande av ny uppdaterad baseline
    - Genomför/rulla ut ny/uppdaterad baseline
    - Scanna/kontrollera genomförandet
      - strul vid installation berorende på fel i baseline
      - lyckad installation - åtgärd försök på nytt
    - Rapportera
      - genomförd installation
      - avvikelser vid installation
      - vidtagna åtgärder
      - erfarenheter/lessons learned
    - Klart
  - Sårbarhetsscanning
    - Definiera
      - vad som ska scannas
        - ip-adressområde
      - hur det ska scannas
        - avvikelser mot organisationens it-security baseline
          - Organisationens krav/behov/styrande dokument styr tekniken, Inte tvärtom!
          - kräver normalt att scanners regler anpassas i enlighet med organisationens it-security baseline
        - scannerns "standardregler"?
        - annat?
    - Planera scanning
      - När/tidpunkt
      - Hur ofta
      - Vad
        - hela nätverket på en gång
        - delar av nätverket
      - Hur
        - icke-inloggad
        - inloggad
    - Genomför scanning
      - strul vid scanning
        - definitionsfel
        - planeringsfel
        - tillfälligt strul
          - scanna på nytt
      - lyckad scanning
    - Scanning - Rådata
      - Exempel

192.168.5.16	CVE-2018-8347	7.8 High	An elevation of privilege vulnerability exists in Microsoft Windows when the Windows kernel fails to properly handle parsing of certain symbolic links, aka "Windows Kernel Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers.

      - Tänk på
        - Detta är endast 1 rad
        - Normalt handlar det om 100 - 10 000 tals avvikelser!
    - Det är först när man har hela bilden som det går att prioritera vad som är viktigast att patcha först...!
    - Bearbeta och prioritera
      - Nödvändigt komplettera med information från olika källor
        - HR-database
        - inventarieregister
        - applikationsregister
        - etc
      - Exempel

Uppgifter som scenarern ÖJ känner till MEN som behöver utredas för att kunna utföra arbetet med att prioritera och åtgärda avvikelsen samt även för rapportering efter utförd åtgärd	
Org Enhet 1	ACME XX
Org Enhet 2	Företagskunder
Kostnadsställe	120056
Application Owner	Carl Kalender
Application	Prosit
Customer Facing	Ja
Internet Facing	Ja
GDPR	Ja
Verksamhetskritisk	Ja
24/7/365	Ja
Fall Back	Nej
Application Provider	Anna Larsson
UtrustningID	45329302
Inventarienummer	IT6-27401
Tillverkare	Microsoft
Produktgrupp	Operativsystem
Produkt	Windows Server
Version	12.8

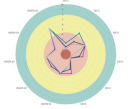
Sammanställning av koncernsäkerhetsstatus	
Sammanställning av bolagets säkerhetsstatus	
Vem tar kostnaden för arbetet?	
Problemägare. Beslut om åtgärder för åtgärd.	
Vad är det för system som körs på maskinen?	
Vad har applikationen/utrustningen för exponering?	
Vad har applikationen/utrustningen för exponering?	
Har är skadekostnaden med avseende på GDPR?	
Har är skadekostnaden med avseende på verksamhetens?	
Har är skadekostnaden med avseende på driftstopp?	
Finns det kontaktande eller backup-maskiner? (så fall vilka (för patchning även av dem)	
Intressent - behöver känna till patchen så den inte medför oönskade driftsstörningar	
Var finns utrustningen?	
Har gammal är utrustningen? Är det bättre att ersätta den?	
Vem är tillverkare/leverantören?	
Vad är det för vägar? (operativsystem/databas/härdnorm/etc)	
Vad är det för produkt?	
Vilken version? (Speciellt viktigt/användbart att veta i de fall en Security Advisory från en leverantör anger att version x måste uppdateras)	

      - Utför korrigerande åtgärder dvs Patcha
        - Planera
        - Genomför
        - scanna/kontrollera
        - rapportera
    - Rapportera - informations/beslutsunderlag
      - Högsta ledningen

Företagsledningen – endast övergripande rapport

Status Hög risk avvikelser - Företag Acme XX		
	Denna månad	Föregående månad
Totalt antal hög risk avvikelser	3006	2832
Risktoleranstal	450 – 880 MW	440 – 1090 MW
Genomsnittlig åldrar på avvikelser	825 dagar	980 dagar

Inte bara text, även grafik, t.ex. pajdiagram/spindeldiagram eller andra typer av diagram som stöpsel etc



      - Enhetschefer

Enhetschefer – övergripande info avseende deras enhet samt möjlighet att jämföra sig med övriga enheter

	Icke-Föreläg	Icke-och nivåer	Privatkunder	Offentlig	IT-drift
Totalt antal avvikelser	xxxx	xxxx	xxxx	xxxx	xxxx
Antal hög-risk avvikelser	492 (503)	510 (505)	535 (502)	562 (562)	587 (590)
Genomsnittlig ålder på avvikelser	890 dagar	1209 dagar	336 dagar	854 dagar	727 dagar
Applikationer – topp tre - avvikelser	Smart, Bok, CRM	CRM, Guld, Rex	Bok, Privat, Smart	Inv, pc, Rex	Nessus, AD, SSO

      - Utförarrapport

Utförarrapport

Till varje grupp, anpassad info med den info de behöver. Detta som en del i processen, det verktyg de behöver för att kunna jobba effektivare och slippa lägga mycket tid på att ta reda på exakt vad som behöver göras.

Ansvar	Ip-adress	Avvikelse	Åtgärd	Tid	Övrigt
Unixgruppen	192.168.1.12 192.168.4.25 192.168.4.26 192.169.4.40 192.165.4.55 etc	CVE-xxxx-xx	Installera uppdatering enligt leverantörens rekommendation xxxx	2018-12-14:00:00 – 2018-12-14:07:00	Kräver omstart
Windowsgruppen	192.168.1.10 192.168.2.25 192.168.2.26 192.169.3.40 192.162.2.18 etc	CVE-xxxx-xx	Orinnistallera xyz	ok att göra när som helst	Kräver ej omstart.
Skrivargruppen	192.232.1.20	Skrivare x sönder	Ta ur hårddisk ur skrivaren. Skicka skrivaren på service hos leverantör (namnk. Adress: xxxx.		Placerad, hus x, vån 3, rum 32
Databasgruppen	192.168.14.20	CVE-xxxx-xx	Omstart av xxx	2018-12-12:02:00 – 2018-12-12:08:00	