SUNET säkerhetscenter

Ransomware en risk för din organisation?

David Heed, IT-säkerhetssamordnare

Vetenskapsrådet

SUNET

Agenda

- Nuvarande hotbild
- Vad är Ransomware
- Hur fungerar det
- Tidigare attacker
- Best practise och Motåtgärder
- Hur hanterar man en incident om det ändå inträffar
- Diskussion och frågor

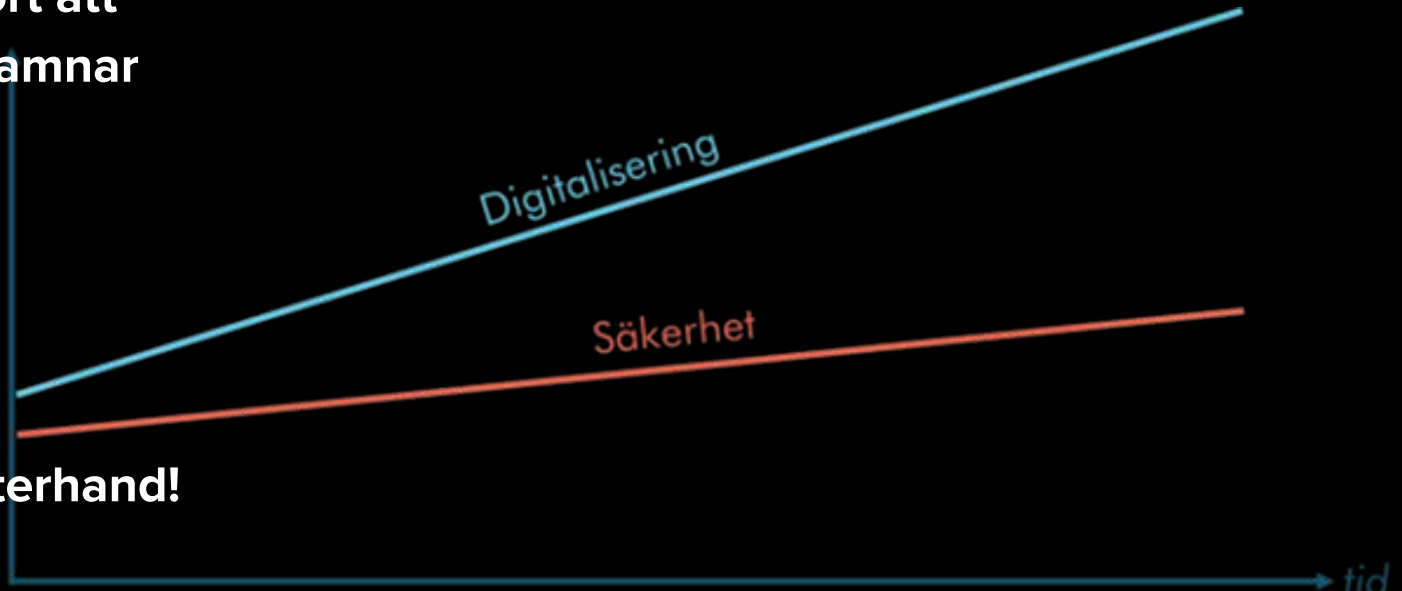
Säkerhetsområdet har växt

- Informationssäkerhet
- IT-säkerhet
- Dataskydd
- Fysiskt skydd
- Medarbetarkompetens

- Legala krav
  - Granskning, styrning och kontroll
  - Leverantörsstyrning och kravställning
  - ev. Säkerhetsskydd, Totalförsvar
  - NIS2…. (Stor osäkerhet kring implemeringskrav)

Säkerhetsområdet måste ges resurser

En allt snabbare utvecklingstakt & digitalisering har gjort att säkerhetsområdet hamnar efter...



Teknisk skuld är dyrt att räta upp i efterhand!
Incidentkostnad x10

En förändrad hotbild enligt Säkerhetspolisen

Från Säkerhetspolisens årsbok 2020

- *“ […] Säkerhetspolisen bedömer att underrättelsehotet kommer att fortsätta vara högt de närmaste åren. Det kommer främst att rikta sig mot kommersiella mål, militära mål, teknik, forskning och utveckling och mot människor som sökt fristad i Sverige.”*
- *“ […] Angreppen riktas bland annat mot svensk världsledande forskning och innovation med målet att stjäla kunskap och ta över företag för att olovligen bygga kompetens och förmåga. Säkerhetspolisen uppskattar att den information och kunskap som olovligen inhämtas varje år kan värderas till miljardbelopp.“*
-

Från Säkerhetspolisens årsbok 2022

- *“ […] I andra fall använder de sig istället av externa bolag eller universitet, detta för att göra det svårare att koppla angreppen till den stat som utfört angreppet”*
- *“ […] Konsekvenserna av den omfattande kinesiska inhämtningen mot svenska företag och forskningsinstitutioner riskerar att dränera Sverige på innovationsförmåga och konkurrenskraft”*

Vetenskapsrådet

SUNET

Huvudsakliga trender enligt ENISA

- Nyupptäckta sårbarheter (Zerodays) är den nya resursen som används av hotaktörer för att uppnå sina mål
- En ny våg av hacktivism har observerats sedan kriget mellan Ryssland och Ukraina
- DDoS-attacker blir större och mer komplexa och går mot mobila nätverk och Internet of Things (IoT) som nu används i cyberkrigföring

Källa: ENISA threat landscape 2022

Realiserade hot mot vår sektor

1. **Belastningsattacker**
   - DDoS större nu än tidigare

2. **Återanvändning eller svaga lösenord (inte multifaktor…)**
   - Kan vara en språngbräda in

3. **Phishing av olika slag**
   - Spearphishing som riktar sig mot ekonomi eller it

4. **Senfärdiga systemuppdateringar**
   - Leder till potentiellt till dataintrång och missbruk av resurser

5. **Ransomware** (inga ännu kända stora incidenter i svensk sektor)

Källa: Sunet intern statistik och insamling

Vad är ransomware...?

“Ransomware” är en undergrupp av skadlig kod som ofta låser datorn eller åtkomsten till filerna som finns lagrade eller tillgängliga för användaren eller systemet.

Ofta skapade med drivkraften att tjäna pengar.

Varianten som enbart förstör brukar kallas “Wipers”. Dessa har inte någon ambition att tjäna pengar initialt.

Både Ransomware och Wipers kan ha ambitionen att även stjäla information och kontouppgifter! Om de inte kan få offret att betala för att få tillbaka informationen, kanske de vill betala för att slippa få den exponerad (dubbel-utpressning)

Hur kommer de in egentligen...?

Utnyttja befintliga inloggningsuppgifter (phishing eller skadlig kod)

Utnyttja sårbarheter inom tekniska plattformen (intrång)*

*Kanske vanligare i Sverige med angrepp via stulna konton än intrång?

(finns många olika datakällor men ingen samlad bild)

Hur fungerar ransomware

Programmen är moderna datavirus med ett syfte annat än skada.

- Initial infektering
- Inventering av närliggande system/spridning
- Kryptera alla tillgängliga resurser (G:\ ..... ?)
- Inväntande av inloggningsuppgifter/credentials
- Spridning mellan system

Direkta och indirekta kostnader

Genomsnittligt utpressningsbelopp för Ransomware 2023 är $1 540 000
Detta är nästan en dubblering från 2022 ($812 380)*

Indirekta kostnader:
Stillastående organisation (x anställda, x studenter m.m.)
Förlorat förtroende och kanske missade deadlines?
Förlorat forsknings och verksamhetsdata?
Teknikskuld och återställningskostnader

Hur kan man hantera ransomware?

Två val

1. Betala.... (inte rekommenderat)
2. Återställ från säkerhetskopior

(mer info senare)

Hur påverkar ransomware företag

“93 percent affected companies without a Disaster Recovery plan closed down businesses within one year of the data attack.”

“96 percent of companies backed by Disaster Recovery was able to tackle ransomware attacks.”

Vetenskapsrådet

Source: https://www.veritis.com/blog/disaster-recovery-2019-statistics-insights-that-shape-your-business-future/

SUNET

Exempel på attacker

2023
Unauthorized access at U.S. e-learning provider
3rd Millennium Classrooms - Austin, Texas, USA (Travis County, Hays County, Williamson County)

Student and alumni data subject to information security breach
https://www.cavalierdaily.com/article/20...

October 2023
Unauthorized access at a college in Israel
Kiryat Ono / קִרְיַת אוֹנוֹ, Israel

Billboards in Israel were briefly hacked to display pro-Hamas messages as cyberwar ramps up
https://www.cnbc.com/2023/10/12/billboar...

October 6, 2023
Cyber attack on a hospital in Germany
Universitätsklinikum Frankfurt - Frankfurt/Main, Hesse, Germany

Hackerangriff auf Uniklinik in Frankfurt
https://www.faz.net/aktuell/rhein-main/f...

October 2, 2023
Cyber attack on a university of applied sciences in Germany
Hochschule Karlsruhe (HKA) - Karlsruhe, Baden-Württemberg, Germany

IT-Infrastruktur der HKA Ziel eines Cyberangriffs
https://h-ka.statusinfo.live/

Cyberangriff auf Karlsruhes Hochschule: Für Studis ging der Unterricht am Mittwoch trotzdem weiter
https://www.ka-news.de/region/karlsruhe/...

September 28, 2023
Security incident at the IT operator of a university in Germany
Gesellschaft für wissenschaftliche Datenverarbeitung - Göttingen, Lower Saxony, Germany

Sicherheitsvorfall 28.9.2023 – Update 1 – Aufruf zur Passwortänderung
https://status.gwdg.de/incidents/80875

Hackerangriff auf die GWDG: Beschäftigte der Uni Göttingen müssen Passwörter ändern
https://www.goettinger-tageblatt.de/loka...

September 2023
Cyber attack on a college in New York City
Baruch College - New York City, New York, USA

Baruch closed for the remainder of the week amid malware attack
https://theticker.org/12226/news/breakin...

Maastricht dec 2019

Väldokumenterad attack

Efterspelet....

€500 000 i kryptovaluta kunde omhändertas

Styrelsebeslut att återanvända pengarna för att assistera studenter

Maastricht University

Vetenskapsrådet

SUNET

Ålborgs universitet 2020

NYHED

IT CRIMINALS HAD ACCESS TO A FEW USERS' SENSITIVE INFORMATION

LAGT ONLINE: 03.09.2020

A quick reaction from Aalborg University (AAU) meant that only a few employees' sensitive personal data was compromised when IT criminals hacked into Aalborg University's IT system. This is the result of the investigation initiated by AAU immediately after the shutdown on August 4th. The compromised data concerns salary information of 28 employees or former employees, and passwords of 15 students and employees. Those affected are now being informed in a letter.

Exempel: Kalix kommun dec 2021

Tidigare presenterad på Sunetdagarna

Orsak: Angripare agerade inom verksamheten, krypterade information

Återställning kunde ske och investeringar kring två-faktorsinloggning infördes som en tidig åtgärdsinvestering

Exempel: COOP juni 2021

Supply chain attack

Orsakad av dålig programmering av autentisering

(inloggningsfunktion)

Exempel: CloudNordic augusti 2023

Bristfällig incidenthantering och skydd av säkerhetskopior.

Resultat: All data förstörd för alla kunder = konkurs.

Home > News > Security > Hosting firm says it lost all customer data after ransomware attack

Hosting firm says it lost all customer data after ransomware attack

By Bill Toulas August 23, 2023 10:40 AM 8

Danish hosting firms CloudNordic and AzeroCloud have suffered ransomware attacks, causing the loss of the majority of customer data and forcing the hosting providers to shut down all systems, including websites, email, and customer sites.

The two brands belong to the same company and stated that the attack unfolded last Friday night. However, today's operational status remains highly problematic, with the firm's IT teams only managing to restore some servers without any data.

Variant på attack: utnyttja sårbarheter

En stor del av de attackerna sker via dataintrång.

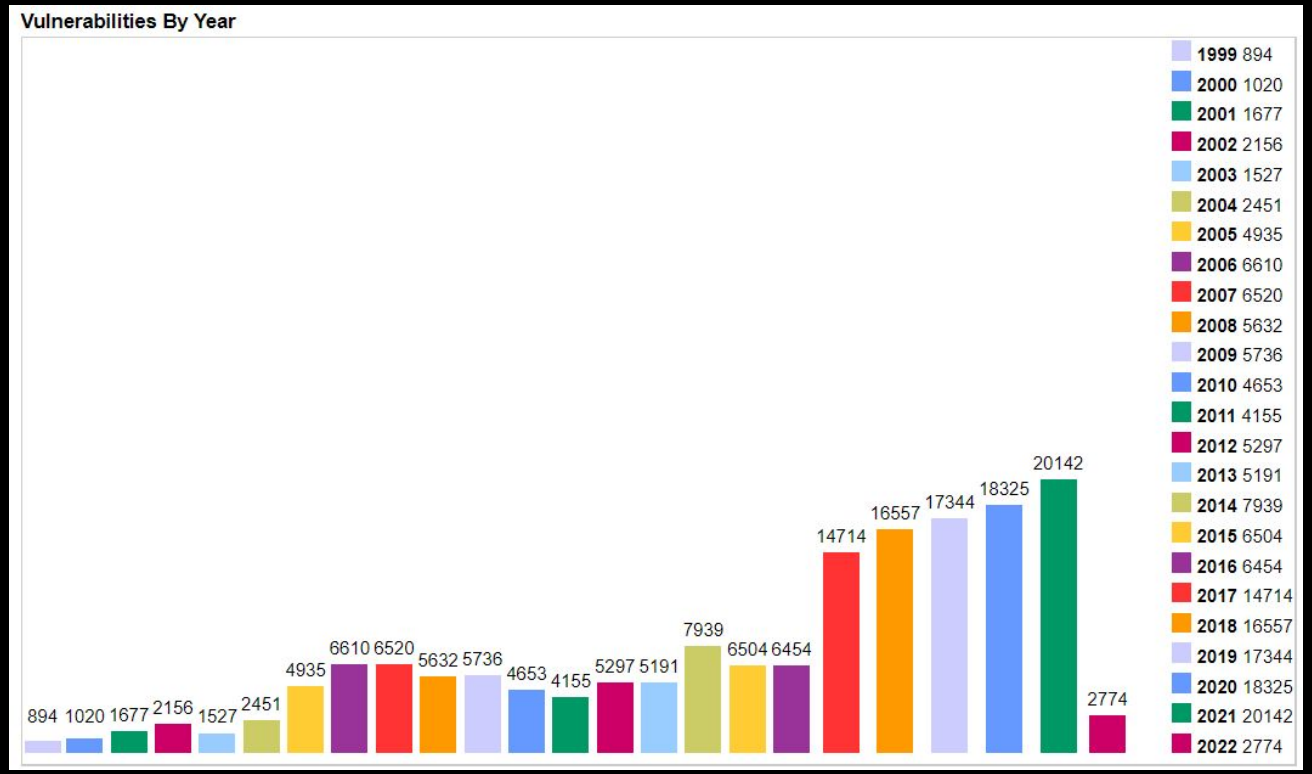
En enda sårbarhet i ett exponerat system kan bli en språngbräda!

- Når andra system direkt
- Spelar in lösenord som används
- Exfiltrerar data som är tillgängligt

På senare tid vanligt med system som exponeras mot internet så som VPN, Citrix m.m.

Ett växande antal sårbarheter

2023 växer det med över 2000st varje månad



ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000										1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000					5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux		4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux				5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win		5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 © zerodium.com

Vetenskapsrådet

SUNET

Verifiera sårbarheter

SUNET utför automatiserade scanningar

Kritiska sårbarheter som finns för vanligt förekommande system av högt värde utförs särskilda scanningar av

SUNET kan också genomföra säkerhetsgranskningar mot egenutvecklade system och utifrån er miljö!

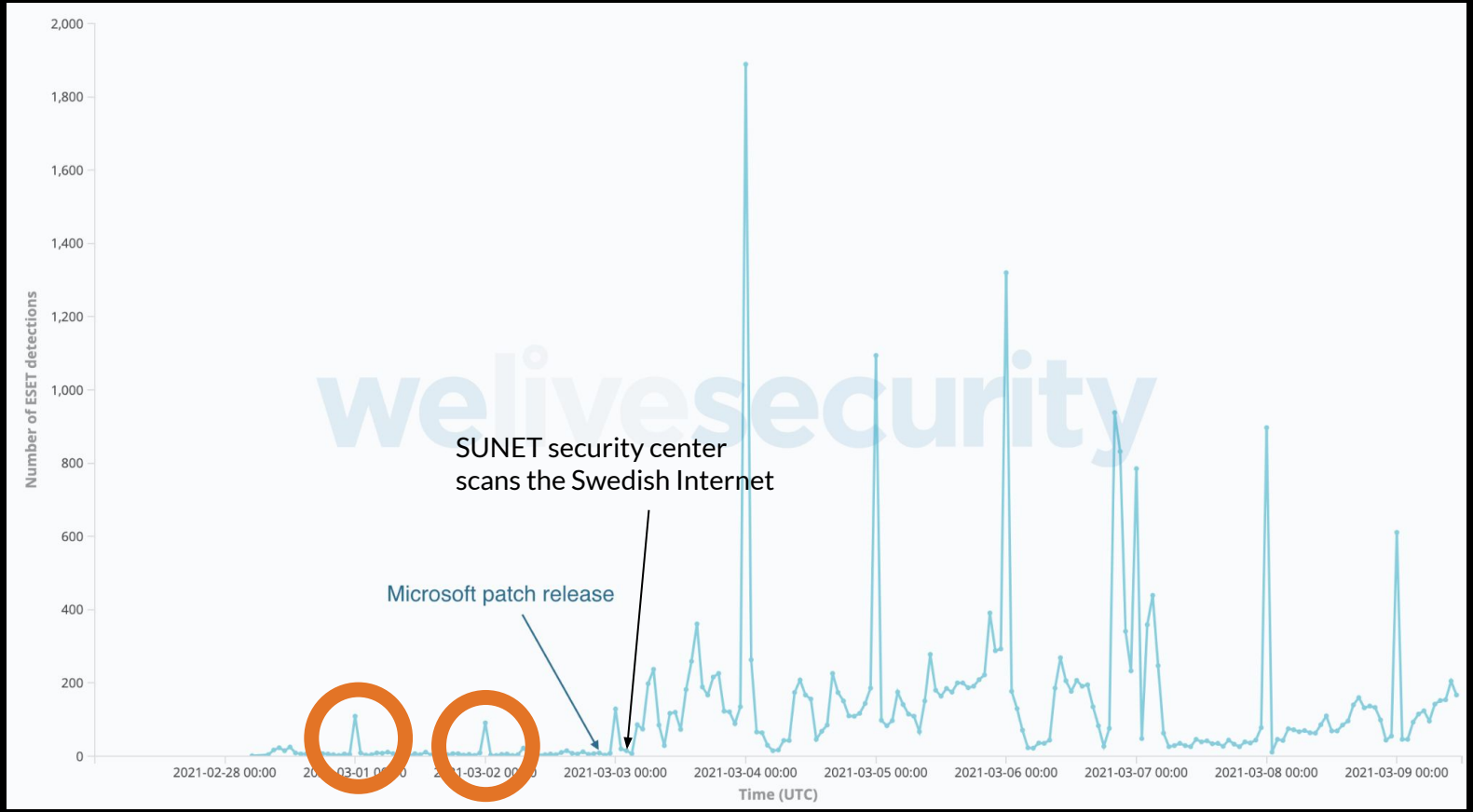
Olika typer av säkerhetsgranskningar

- Sårbarhetsscanning (ofta automatiserad “fördefinierat resultat”)
- Penetrationstestning (ofta manuellt, kan vara fysiskt och socialt, byter ibland riktning)
- System granskning/audit (kombinerar automatiserad och manuella)
- Övergripande säkerhetsgranskning (genomlysning, ofta utöver tekniken)
- Risk och sårbarhetsanalys (grupparbete för att prioritera ändringar och motåtgärder)

Everyone gets redteamed daily, not everyone gets the report... =)

Syftet med IT-säkerhetsarbetet är att så långt som möjligt *förebygga* framgångsrika IT-attacker mot Sunet och våra kunder

Lyckat exempel: Kortad ledtid MS Exchange

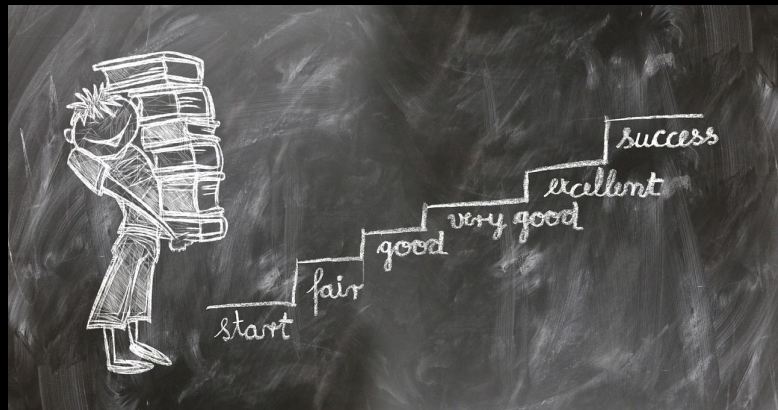


Prioriterade åtgärder för it-ansvariga

10 st förslag på åtgärder.

Prioriteringar beror på omständigheter och detta är allmänna råd, inte en checklista.

Sunet Säkerhetscenter finns till för er som anslutna organisationer och kan assistera med rådgivning och koordinering av incidenter. Helst genom att undvika problemen genom proaktiva åtgärder!



Säkerställ att ni har en fungerande säkerhetskopia

Genomför systemåterläsningstester tillsammans med verksamheten.
Var inte nöjd som it-avdelning att systemet startar

- Finns rätt data?
- Är all data tillgänglig?
- Fungerar andra integrationer och beroenden?

Offline (gärna offsite) säkerhetskopior, annat media/operativ system

Skilj på backup och restore både som konto och rättighet

Segmentera nätverket

Tiers

Systemtyper

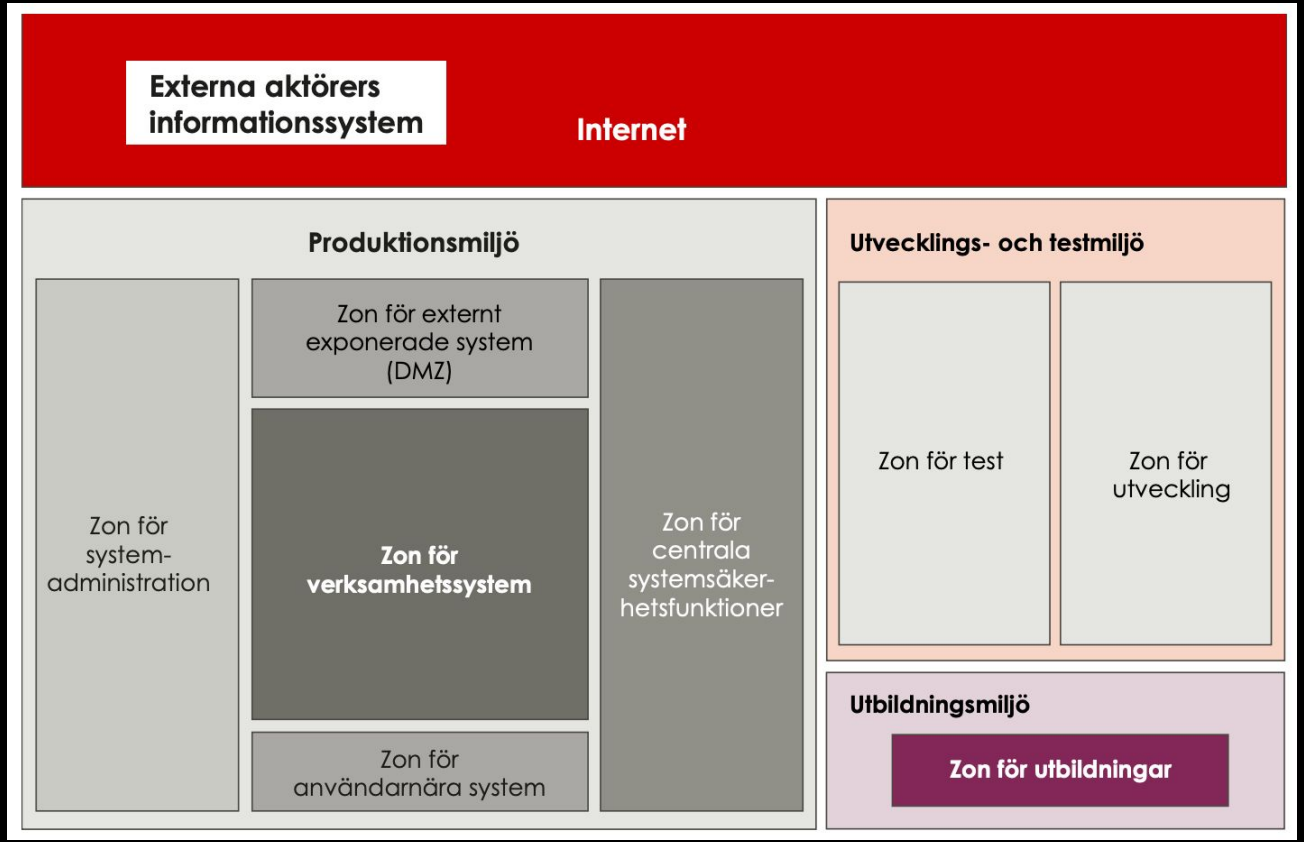
DMZ

Åtkomst:

VPN

Proxy

Split horizon DNS



Exempel: MSBs vägledning nätverks indelning

Installera säkerhetsuppdateringar skyndsamt

Andra tisdagen varje månad släpps vanligen flera kritiska uppdateringar för Windows

Oday (nya sårbarheter) kan upptäckas dagligen.

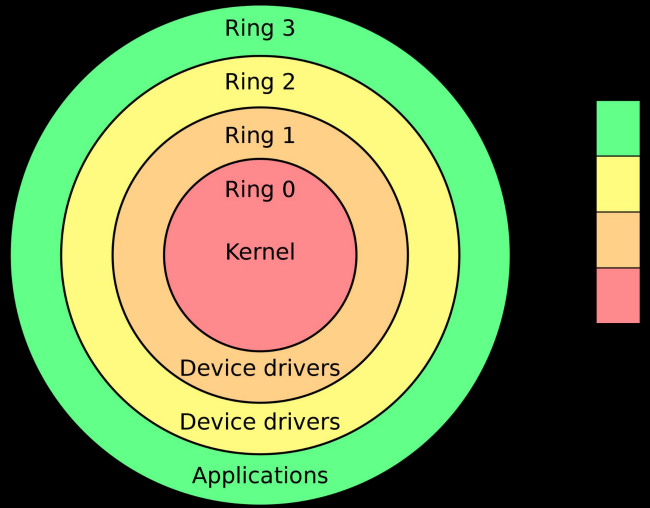
Var vaksam och följ våra rekommendationer och utskick

Begränsa behörigheter

Begränsa behörigheter till relevanta roller,

Servicekonton bör endast ges
tillgång till det de specifikt skall utföra
(inte med systemrättigheter)

Dela inte ut allmänna skrivrättigheter
i stora utdelningar



Härda systemen

Guider

Best practise

Automation (GPO, templates)

Compliance controls

= Stäng ned onödiga tjänster och inställningar

Skydda privilegierad konton

Tier

Admin

Klient

Nätverk

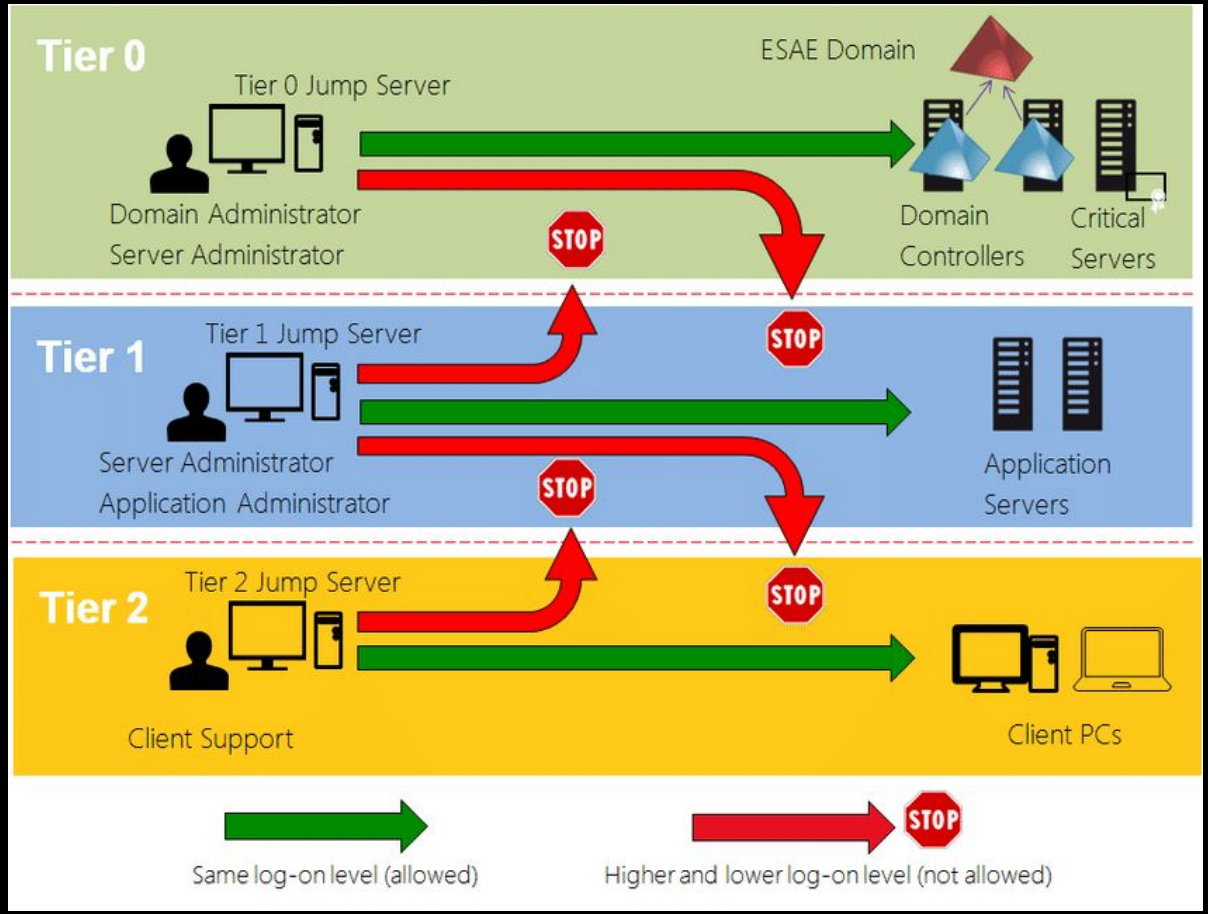
Border / OOB

Hierarkisk administration

Skilj på konton

Skilj på miljöer

Skilj på åtkomst mellan



Tillåt endast godkänd utrustning i nätverket

Asset inventory

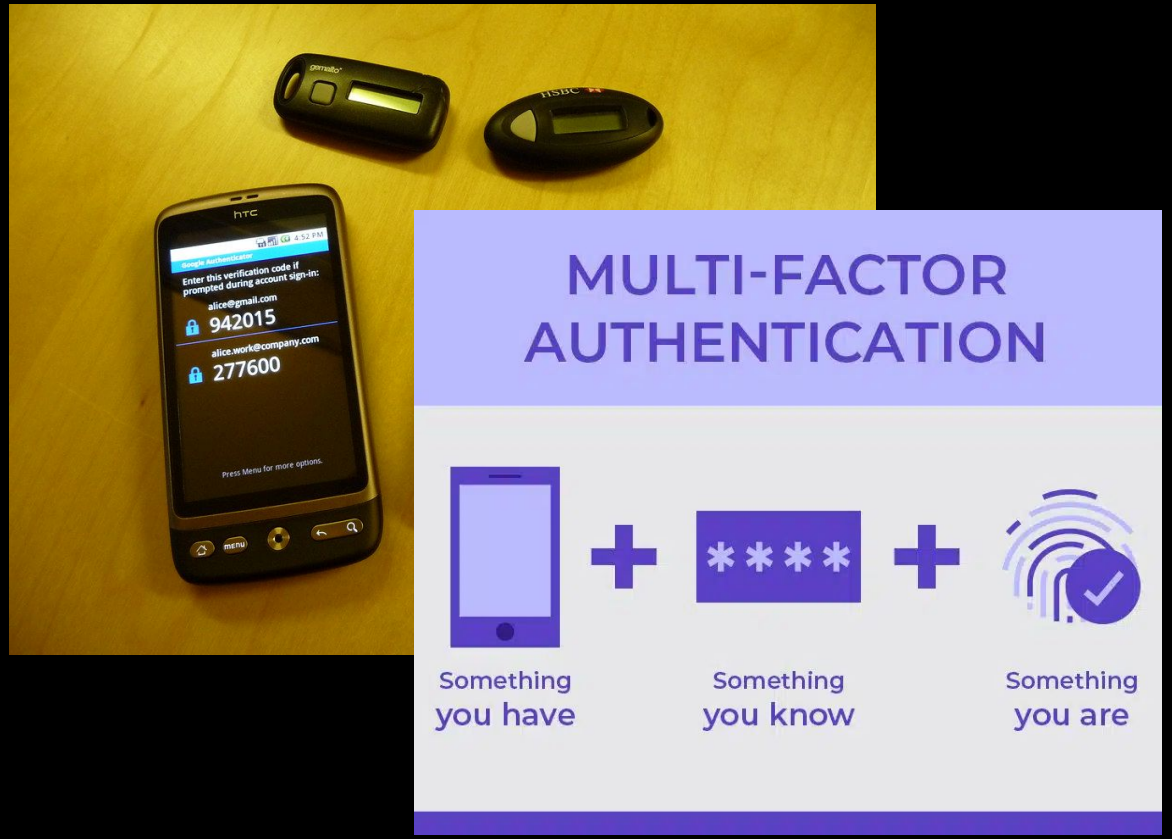
Policy och riktlinjer

Öppna gästnätverk

Aktivera multifaktorsinloggning

MFA

Authenticator



Genomför utbildning i informationssäkerhetsmedvetande

En relativt billig åtgärd är att regelbundet träna och informera medarbetare om vaksamhet mot bedrägeriförsök och att alltid kontakta servicedesken vid “konstiga rutor”.

Testa och öva er säkerhet

Säkerhetsgranskningar och penetrationstester

Krisövningar

Summering - Prioriterade åtgärder för it-ansvariga

- Säkerställ att ni har en fungerande säkerhetskopia
- Segmentera nätverket
- Installera säkerhetsuppdateringar skyndsamt
- Begränsa behörigheter till relevanta roller, inte allmänna skrivrättigheter i stora utdelningar
- Inaktivera oanvända tjänster och protokoll (härda systemen)
- Separera och skydda användningen av högre rättigheter
- Tillåt endast godkänd utrustning i nätverket
- Aktivera multifaktorsinloggning, återanvänd inte lösenord
- Genomför utbildning i informationssäkerhetsmedvetande
- Testa och öva er säkerhet, skall vi....?


Everyone has a plan 'till they
get punched in the mouth
Mike Tyson

Under en pågående incident (för IT-chefen)

1. Identifiera påverkan och begränsa fortsatt skada
2. Eskalera och kommunicera till krisorganisationen lokalt
3. Prioritera återställande av kritiska system och gemensam infrastruktur
4. Återställ data
5. Övervaka stabilitet, nyttjande och loggar
6. Kommunicera, kommunicera, kommunicera

Se till att personalen har något att äta, men skicka hem dem om det blir för sent. Tro inte att man kan genomföra arbete dygnet runt under flera dygn.

Under en pågående incident (för IRT)

1. Incidenthanteringprocess, eskalering till krisläge(?)
2. Begränsa skada
3. Förebygg fortsatt spridningsförmåga
4. Eliminering av Ransomware
    - Isolering av resurser, ominstallation Domän kontrollanter, återbyggnad av GPO m.m.
    - Byte av lösenord (användare och system)
    - Återställning kritiska system och gemensam infrastruktur
    - Återställning viktiga system
    - Återgång till det normala
    - (glöm inte lokala konton och statiska konfigurationer)
5. Dokumentera alla åtgärder löpande

Troligtvis behövs experthjälp från erfarna it-säkerhetsspecialister

Frågor?

Synpunkter!

Kommentarer?

Annat?

Kommande aktiviteter (inom Säkerhet)

Tisdag	13:00	Mailfilter
Torsdag	10:00	eduSign
Torsdag	11:00	Certifikat (TCS)

Sunet säkerhetsdagar 24-25 oktober (Hybridmöten, några fysiska)

- CSIRT-forum, Workshop kring webshells
- Föreläsningar: Säkra AD, hantering av sårbarheter m.m.