IT-säkerhet

Johannes Hörnberg
Verksamhetschef
IT Västerbotten

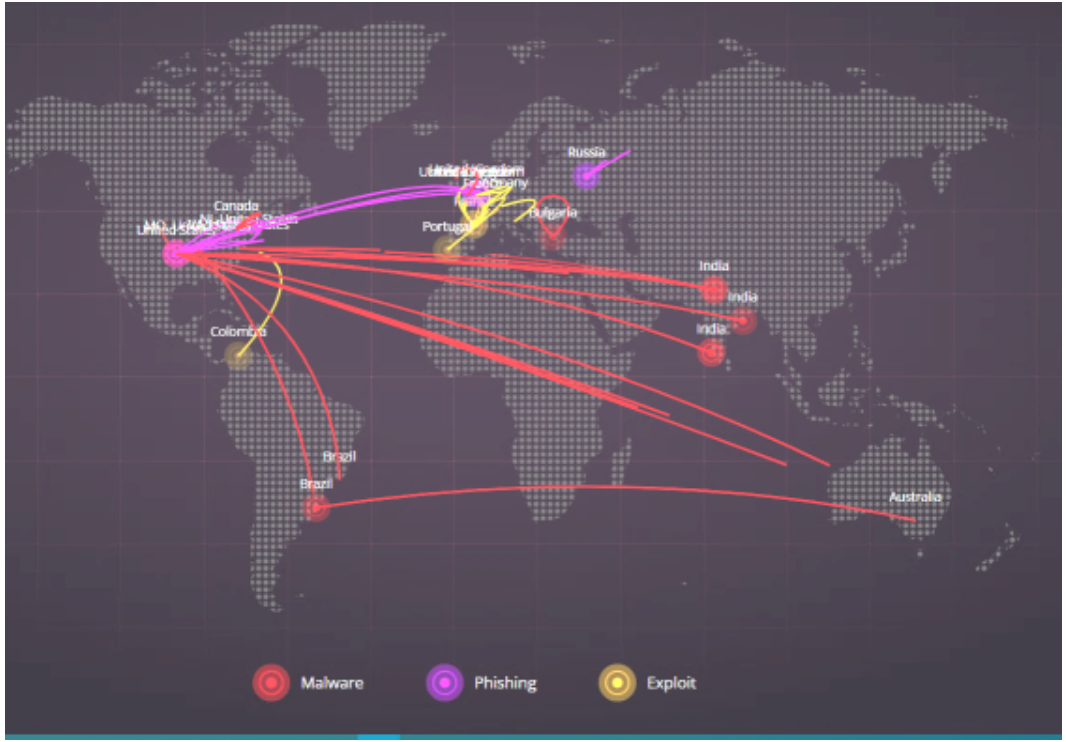
region västerbotten

Agenda

- Introduktion
- Informationssäkerhet
- IT-säkerhet
- Frågor

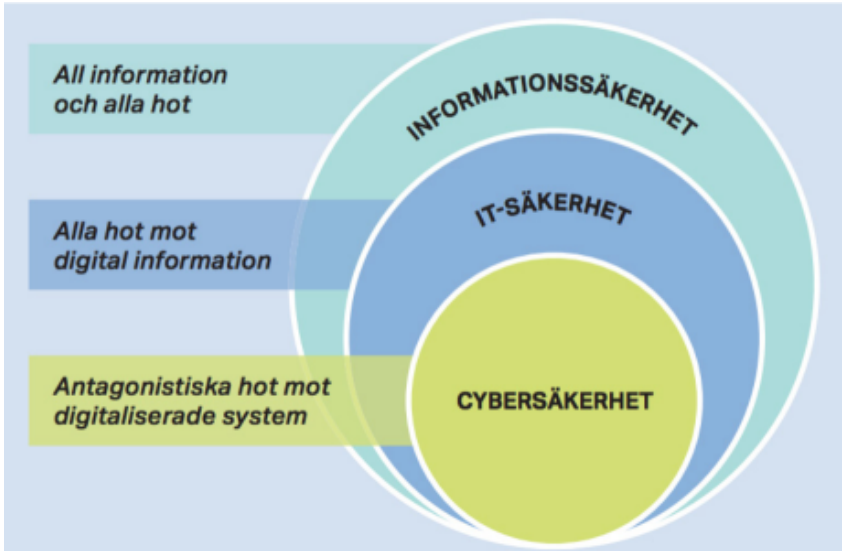
region västerbotten

Hotbilden



region västerbotten

Introduktion



Källa: Teknikföretagen 2020, https://www.teknikforetagen.se/ globalassets/i-debatten/publikationer/cybersakerhet/cyberhoten-motsvenska-teknikforetag.pdf#page=Cyberhoten%20mot%20svenska%20 teknikf%C3%B6retag

region västerbotten

GDPR

Alla verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter. Det gäller oavsett om det är en offentlig myndighet, ett privat företag, en förening eller någon annan typ av verksamhet.

Dataskyddsreglerna grundar sig i de mänskliga rättigheterna. Alla människor har rätt till respekt för privat- och familjeliv och till skydd av sina personuppgifter

region västerbotten

Dataskyddslagstiftning

Region Västerbotten har att följa vad som framgår av bland annat dataskyddsförordningen och den nationella kompletterande dataskyddslagen.

Regionen måste till exempel följa ett antal grundläggande principer, identifiera rättslig grund för behandling, tillvarata registrerades rättigheter, utföra konsekvensbedömningar och förhandssamråd samt säkerställa att överföring till tredje land sker på ett lagenligt och säkert sätt.

region västerbotten

Patientdatalagen

Vad gäller enligt Patientdatalagen och HSLF-FS 2016:40?

- Bibehålla sekretess i systemen
- Korrekt behörighetstilldelning
- Loggning och kontroll av åtkomst i systemen
- Informationssäkerhetspolicy skall finnas
- Krav på att en eller flera personer skall utses för att leda informationssäkerhetsarbetet
- Årlig granskning
- Krav på systemdokumentation
- Krav på säkerhet gällande informationssystem

Informationssäkerhet

Informationssäkerhet handlar i grund och botten om att säkerställa en kontinuitet i upprätthållandet av informationens konfidentialitet, riktighet och tillgänglighet. Inom hälso- och sjukvård ska det även finnas en spårbarhet när det gäller vem som exempelvis har tagit del av, eller ändrat information.

Exempel på krav gällande informationssäkerhet;

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster

- 13 § Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

HSLF-FS 2016:40 …allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården

- 14 § Vårdgivaren ska säkerställa att informationssystem som används för behandling av personuppgifter skyddas fysiskt mot skada, störning och obehörig åtkomst.
- 9 § Vårdgivaren ska ansvara för att;

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient.

region västerbotten

Konfidentialitet

Information varken tillgängliggörs eller avslöjas obehöriga

Riktighet

Information är korrekt och fullständig

Tillgänglighet

Information är åtkomlig och användbar på begäran av en behörig individ, ett objekt eller en process

Spårbarhet

Åtgärder kan härledas till en användare

region västerbotten

Informationssäkerhet i praktiken

Region Västerbotten använder sig av bland annat verktyget KLASSA från MSB för att säkerställa att informationstillgångar ges tillräckligt skydd.

Informationstillgång: Information + den resurs som hanterar informationen, exempelvis ett system och dess innehållande information.

Genom KLASSA kan man dels ta fram upphandlingskrav inför en upphandling och dels skapa handlingsplaner för redan befintliga informationstillgångar.

region västerbotten

Säkerhetsåtgärder för att skydda information

Olika typer av säkerhetsåtgärder;

- Manuella säkerhetsåtgärder (avser administrativa och kunskapsbaserade åtgärder)
- Verktygsbaserade säkerhetsåtgärder (avser fysiska och tekniska åtgärder)

Dessa åtgärder tillsammans i välbalanserat format ger förutsättningar att skydda informationen på ett tillfredställande sätt.

region västerbotten

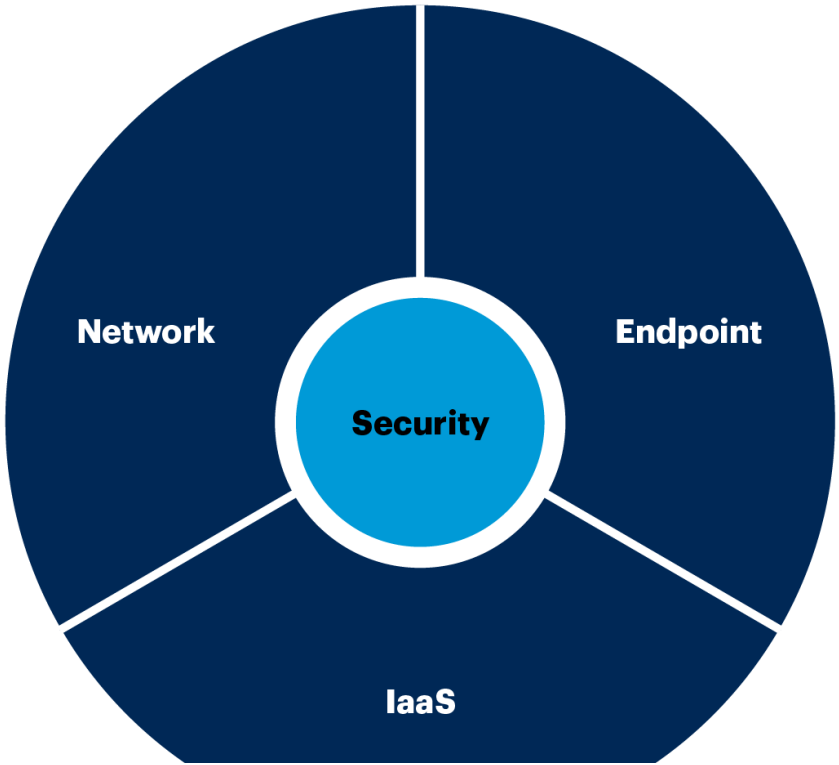
Verktygsbaserade säkerhetsåtgärder

- Att ha tekniska funktioner och verktyg i IT-miljön som kan *skydda*, *detektera* och *analysera* alla olika hotbilder är en förutsättning för en fungerande IT-miljö.

- Region Västerbotten har i dag bra skydd mot virus, ransomware, skadlig kod och nätfiske.

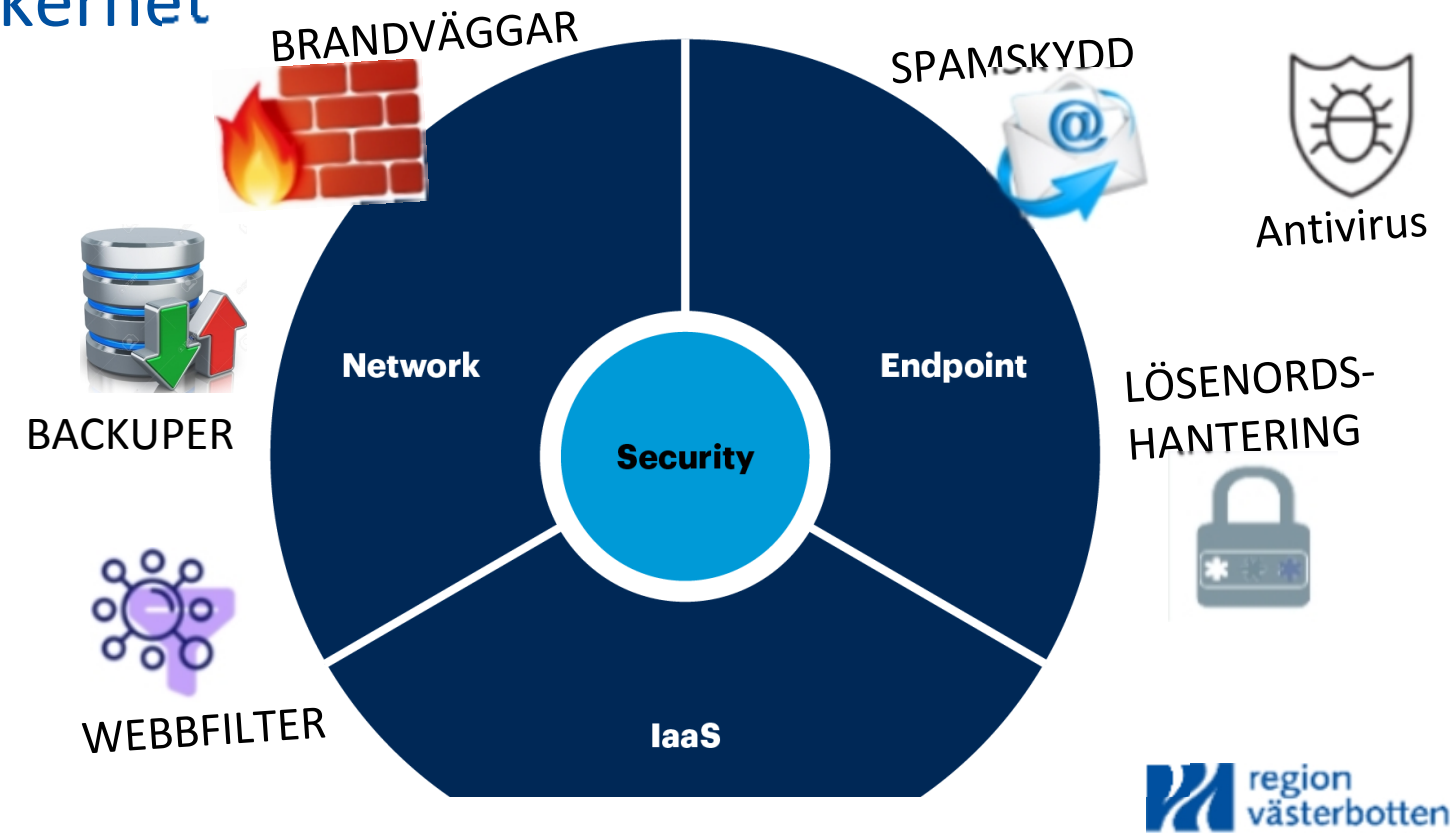
region västerbotten

IT säkerhet

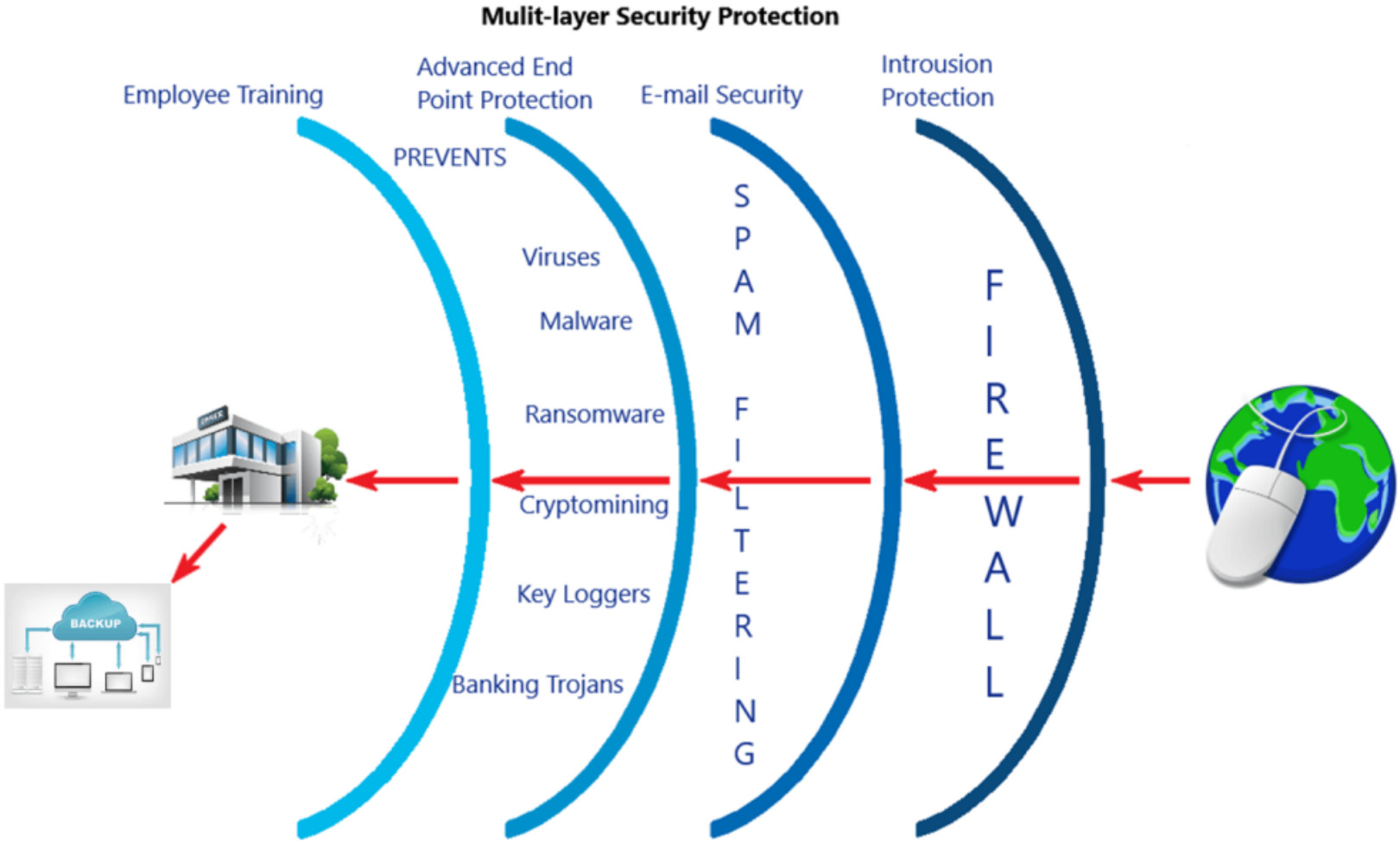


region västerbotten

IT säkerhet



region västerbotten


Mulit-layer Security Protection
Employee Training
Advanced End Point Protection
E-mail Security
Introusion Protection
PREVENTS
Viruses
Malware
Ransomware
Cryptomining
Key Loggers
Banking Trojans
SPAM FILTERING
FIREWALL
BACKUP

Termer och begrepp inom IT säkerhet

Domain		Description
Network Security		Protection of telecommunications infrastructure from threats resulting in compromised data in flight or loss of network availability
Endpoint Security		Protection of endpoint systems, including servers, end-user laptops and desktops.
Data Security		Protection from compromised data, exposed data, loss of data fidelity or lost data resulting from compromised systems, systems failure, or inappropriate user behavior
Identity & Access Management		Protection from unauthorized access to data, applications, and devices, resulting from compromised identities and credentials
Vulnerability Management		Proactive mitigation of risk due to weaknesses, and protection from data exposure and production loss resulting from compromised systems and IT infrastructure
Security Analytics		Use of data analytics captured from security information and events management (SIEM) systems to proactively mitigate risk due to weaknesses in the IT infrastructure
Application Security		Software applications to provide protection from data exposure resulting from transaction compromise or failure
Governance, Risk & Compliance		Protection from security risks through the management and achievement of security objectives commensurate with and necessary for the achievement of business objectives

region västerbotten

Ytterligare åtgärder

- Nedan följer funktioner som ytterligare skulle skydda Regionen mot hot:
  - Fortsatt implementation av tvåstegsverifiering även för inloggning i datorer, nätverk och applikationer
  - Fortsatt segmentering i nätverket
  - Begränsa möjligheten att anslutna enheter i nätverket kan kommunicera med varandra
  - Utöka insamling av metadata från nätverket (Netflow) så att onormala trafikmönster kan detekteras och automatiska åtgärder snabbt kan hindra skada
  - Fortsatt implementation av system för att detektera och stoppa osäkra molnapplikationer (CASB) på datorer och mobila enheter
  - Installera MDM/MEM på tidigare utgivna mobila enheter för hantering/kontroll

region västerbotten

Frågor?

region västerbotten