
RI.
SE
Vi är Sveriges
forskningsinstitut

Sverige kraftsamlar

- RISE bildades för att accelerera Sveriges innovationskraft och skapa bättre förutsättningar för samhällets problemlösare.
- Drygt 30 forskningsinstitut och cirka 130 unika testbäddar har samlats i en organisation.
- Kraftsamlingen ger oss en unik bredd och samlad kompetens.

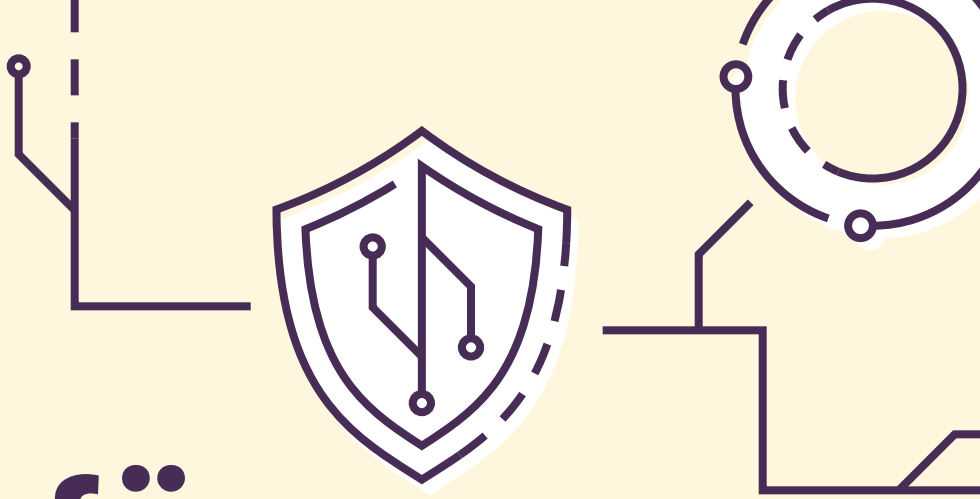
RI.SE

VÅRT UPPDRAG

”Det övergripande målet för instituten inom RISE är att de ska vara internationellt konkurrenskraftiga och verka för hållbar tillväxt i Sverige genom att stärka näringslivets konkurrenskraft och förnyelse, samt främja offentlig sektors förnyelse och förmåga att bidra till lösningar på samhällets utmaningar tillsammans med näringslivet”

Utdrag ur Forskningspropositionen 2020/21:60 Forskning, frihet, framtid – kunskap och innovation för Sverige.Beslutat 21 april 2021

5 samhällsutmaningar som RISE fokuserar på



Centrum för cybersäkerhet

RI.SE

Digitalisering som utmaning och möjlighet
Prop. 2020/21:60

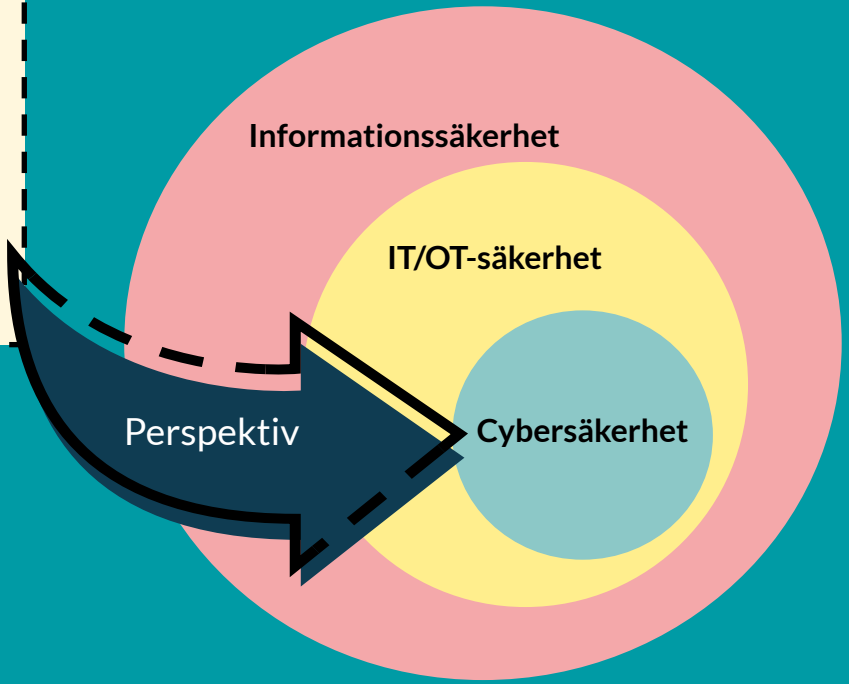
”Målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter behöver samordnas med en förmåga att hantera hot, risker och sårbarheter.”

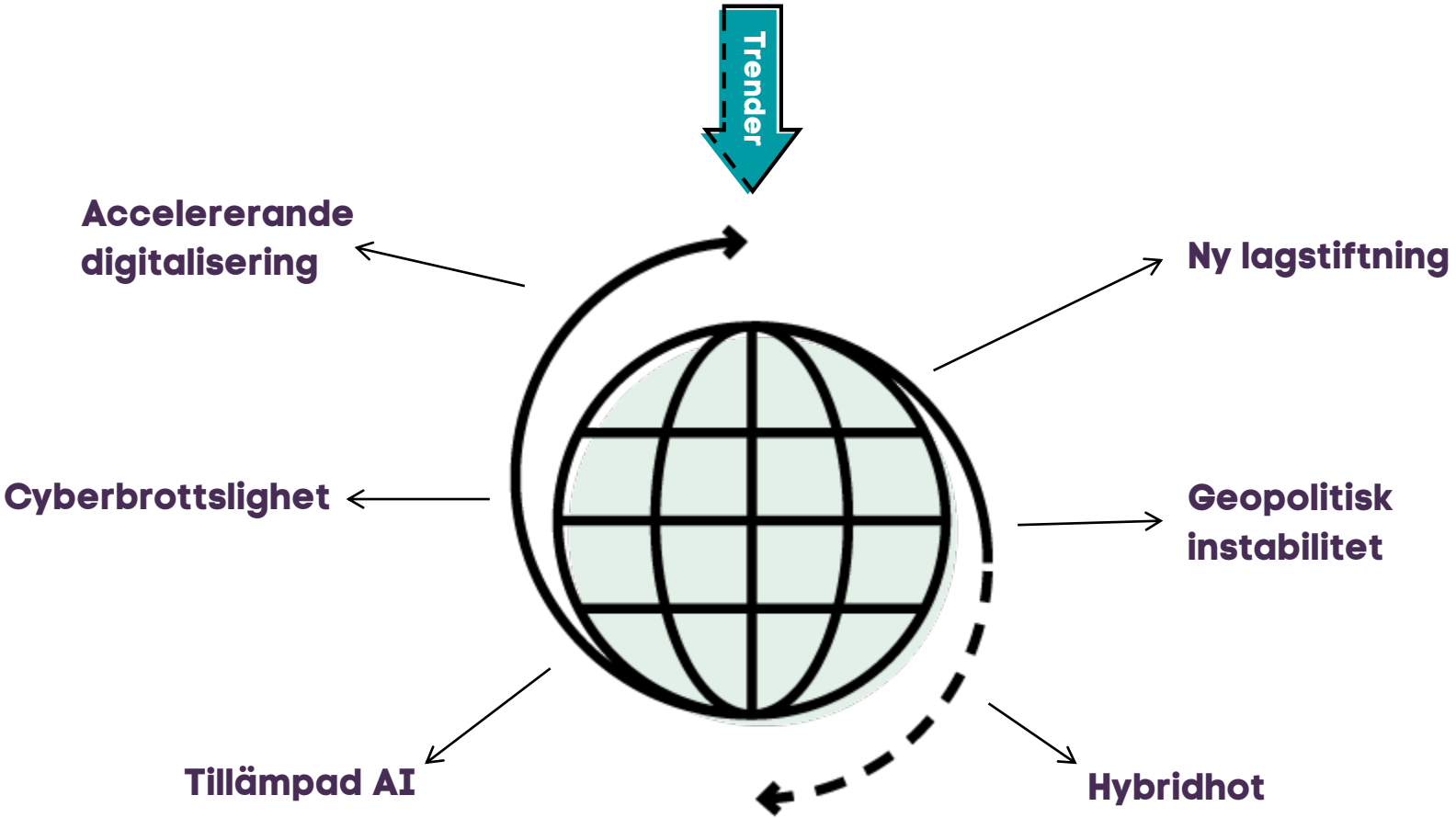
Digitalisering är i sig en samhälls-utmaning, men också både en möjliggörare och sårbarhet i förhållande till övriga utmaningar.

Cybersäkerhet är en förutsättning för att möta samtliga utmaningar på ett robust och framgångsrikt sätt.

Digitalisering som utmaning och möjlighet
Prop. 2020/21:60

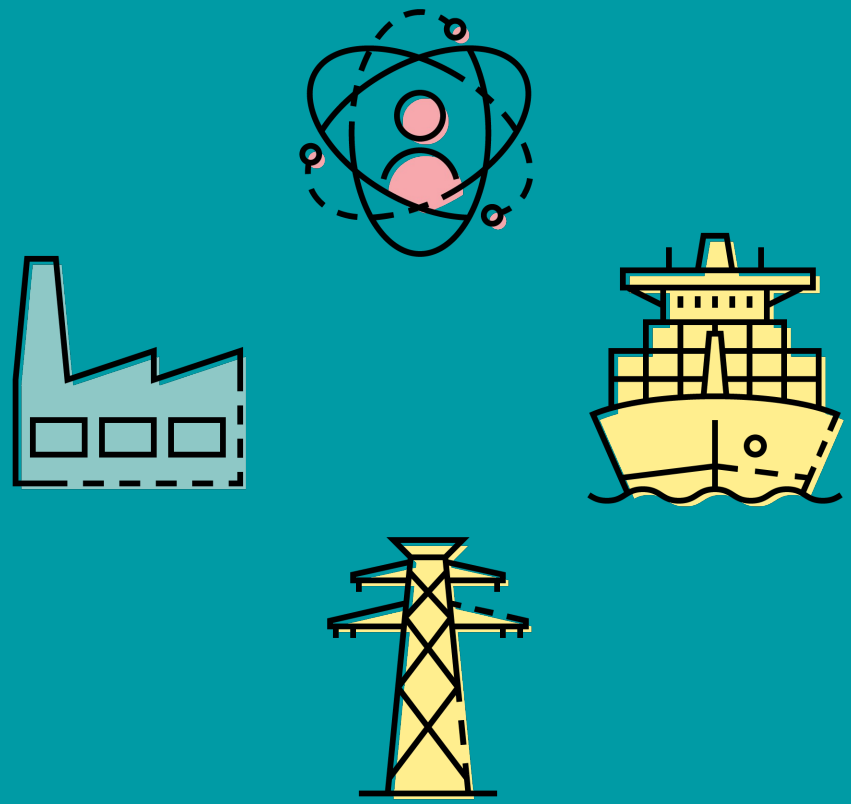
- Teknik
- Ekonomi
- Användare
- Organisation
- Juridik
- Etik
- …




Trender
Accelererande digitalisering
Ny lagstiftning
Cyberbrottslighet
Geopolitisk instabilitet
Tillämpad AI
Hybridhot

Domäner i fokus

- Samhällsresiliens
- Mobilitet
- Energi
- Industri

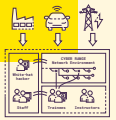


Verksamhet inom cybersäkerhet

Professionell träning & utbildning

Testning av produkter och tjänster

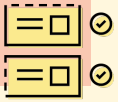
Sektorspecifika digitala tvillingar



Säkra och konfidentiella miljöer

Forskning

Certifiering



Grunderna i cybersäkerhet

RI.SE

Mål

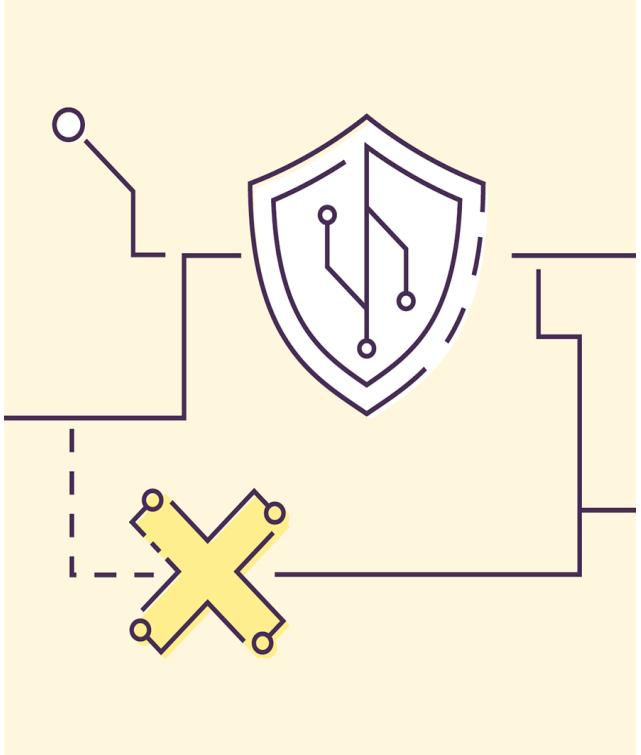
- Ge en förståelse för centrala cybersäkerhetsbegrepp
- Etablera en gemensam vokabulär
- Bekanta sig med vanliga cyberhot
- Lära sig förstå vanliga motåtgärder

Vad är cybersäkerhet?

- Ett samlingsbegrepp för tekniker och metoder för att skydda tjänster, system och nätverk från digitala attacker.
- De digitala attackerna syftar typiskt till att komma åt, ändra eller förstöra känslig information, eller att förhindra åtkomst till digitala system.
- Attackerna kombineras ofta med bedrägerier eller utpressning.

Vad är det vi skyddar?

- Exempel på materiella tillgångar
  - Datorer, nätverk, servrar
  - Produktionssystem
- Exempel på immateriella tillgångar
  - Certifikat, lösenord, kryptovalutor
  - Affärshemligheter, kundregister, bokföring
  - Egna digitala produkter, mjukvara, ritningar, mallar
  - Kundernas data
- Förmågan att leverera.
- Rykte



Cybersäkerhetstriaden

Egenskaper ett system ska ha för att vara cybersäkert

Konfidentialitet

Informationen i ett system är bara tillgänglig för auktoriserade parter.

När det fallerar: Bokslut läcker i förväg till börshandlare.

Riktighet

Information ska inte kunna ändras utan att det går att upptäcka.

När det fallerar: E-post som ändras på vägen.

Tillgänglighet

Ett system eller resurs finns tillgänglig för auktoriserade användare när de behöver den.

När det fallerar: Överbelastningsattack.

Vanliga begrepp

INCIDENT

En händelse som potentiellt hotar säkerheten för ett system eller organisation.

(Man vet inte om någon har gjort något eller om det bara är en tillfällighet.)

INTRÅNG

En situation när säkerheten har brutits, dvs en tillgång har kompromitterats.

(Någon av cybersäkerhetstriadens egenskaper är bruten.)

SÅRBARHET

En brist i mjukvara, hårdvara eller processer som skulle kunna göra att en tillgång öppnas för en inkräktare.

EXPLOIT

Ett konkret tillvägagångssätt som nyttjar en sårbarhet för att komma åt en tillgång.

Vanliga begrepp

CVE - COMMON VULNERABILITIES AND EXPOSURES

En databas över kända sårbarheter i system och mjukvara.

ZERO-DAY

En sårbarhet som ännu inte har dokumenterats i en CVE-databas eller på annat sätt gjorts känd.

PEN-TESTING

Ett test som genomförs för att hitta sårbarheter eller andra säkerhetsproblem i ett system, tjänst eller organisation.

IDS - INTRUSION DETECTION SYSTEM

Ett system som detekterar intrång eller försök till intrång, antingen genom att leta efter kända mönster eller genom att se avvikelser från normalt beteende.

Vanliga begrepp

MALWARE

Ett samlingsbegrepp för skadlig mjukvara.

RANSOMWARE

En typ av malware som låser en tillgång i syfte att utöva utpressning.

SOCIAL-ENGINEERING

Ett samlingsbegrepp för sätt att lura människor, exempelvis för att kringgå säkerhetsmekanismer.

PHISHING

En typ av social-engineering för att få människor att avslöja information, vanligtvis genom e-post.

Vanliga begrepp

KRYPTERING

En matematisk teknik för att göra information oläslig utan nyckel.

Symmetrisk – Samma nyckel för kryptering och avkryptering.

Asymmetrisk – Publik nyckel för kryptering, annan, hemlig nyckel för avkryptering.

DIGITAL SIGNATUR

Ett matematiskt sätt att kunna verifiera riktighet och avsändarens identitet.

Baseras på asymmetrisk kryptering.

HASH-FUNKTION

Ett matematiskt sätt att koppla data till en kort identifierare som inte går att förfalska.

Vanliga begrepp

AUTENTISERING OCH AUKTORISERING

Autentisering – Identifiering av en part.

Auktorisering – Ge en part rättigheter att exempelvis se information.

BOTNET

Ett stort nätverk av datorer som kontrolleras av en hackare.

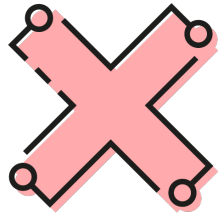
HOT

Sätt som någon kan åstadkomma intrång.

RISK

Konsekvens av intrång (ofta angiven i pengar) multiplicerat med sannolikhet.

Typiska attacker



- Denial of service (DoS and DDoS)
- Social-engineering
  - Phishing, ”tjuvtitta”, infiltration, ”oskyldig” uppmaning
- Malware
  - Virus, Maskar, Trojaner, Ransomware, Spyware
- Man-in-the middle attack
- Web-attacker
  - Injection attacks, Cross-site scripting, Cross-site request forgery
- Supply chain attack
- Lösenordsattacker

Två huvudkategorier av attacker

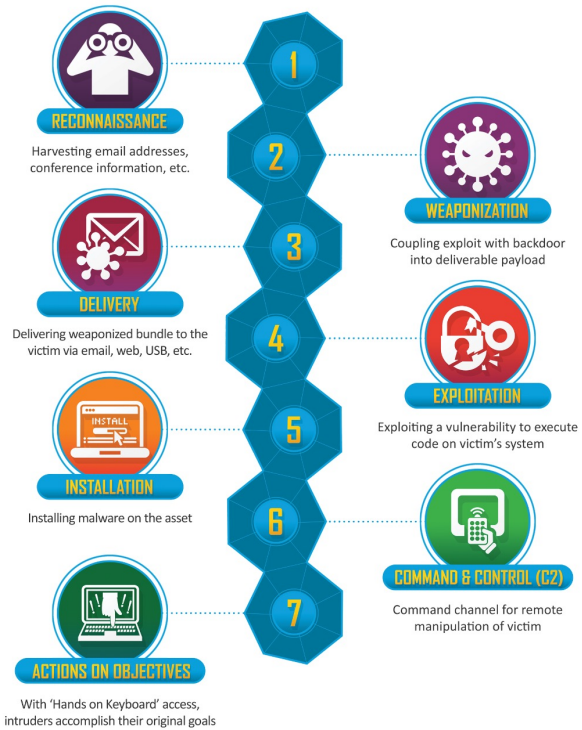
Riktad attack

- Angriparen har valt en tydlig måltavla innan attacken börjar.
- Potentiella svagheter identifieras beroende på det system som angrips.
- Mycket tid och resurser kan spenderas på förarbete och utförande av en attack.

Opportunistisk attack

- Angriparen har valt en sårbarhet istället för en måltavla.
- Angriparen försöker attackera en stor mängd mål.
- Attacker utförs när sårbara mål hittats.

Attack-kedja



Hotaktörer

Cyberbrottslingar – Organiserade grupper eller individer som primärt hackar för att tjäna pengar.

Statligt sponsrade hackare – Hackare som är associerade med stat eller militär i ett land och som primärt hackar för att spionera eller störa viktig verksamhet i andra länder.

Hacktivister – Aktivister som hackar med politiska eller ideologiska mål som att skapa uppmärksamhet eller förstöra för meningsmotståndare.

Insiders – Hackare som själva är associerade med den organisation som de hackar.

Script Kiddies – Ett begrepp för nybörjare inom hackarvärlden som använder verktyg och exploits utan någon större förståelse för dem.

Hackarnas ekosystem

- De hackare som utför en attack är sällan själva utvecklare av de exploits som används.
- Många gånger finns det färdiga verktyg, eller till och med hacking-tjänster att köpa på nätet.
- Detta innebär att även aktörer med begränsad kunskap inom området kan orsaka stor skada.

Skyddsmekanismer

- Segmentering och åtkomstkontroll
  - Nätverkssegmentering
  - Demilitarized Zone (DMZ)
  - Begränsa åtkomsträttigheter
- Autentisering
  - Genomtänkt lösenordspolicy
  - Två-faktors-autentisering
- Nätverkskontroll
  - Restriktiva brandväggar
  - IDS – Intrusion Detection Systems
  - IPS – Intrusion Prevention Systems
- Säkerhetspolicy
  - Regelbundna mjukvaruuppdateringar
  - Säker intern kommunikation

Säkerhetsarbete

- Certifiering
- Verifiering mot standarder
- Penetrationstestning
- Utbildning och träning

Tack!

kim.elman@ri.se