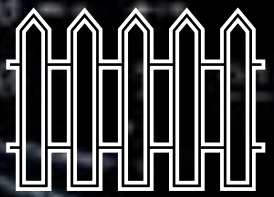
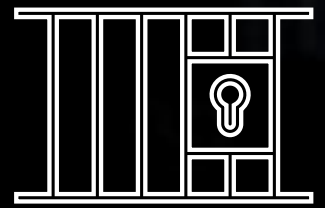
Cybersäkra vattenbrukare, 14 mars 2025

Cybersäkerhet

Skydda din digitala egendom





Hur är läget?

Sverige är ett av världens mest innovativa länder

Sverige är också ett av världens mest digitala länder.

Men ligger inte lika högt inom cybersäkerhet - det gapet behöver vi stänga!

Global Cybersecurity Index 2020

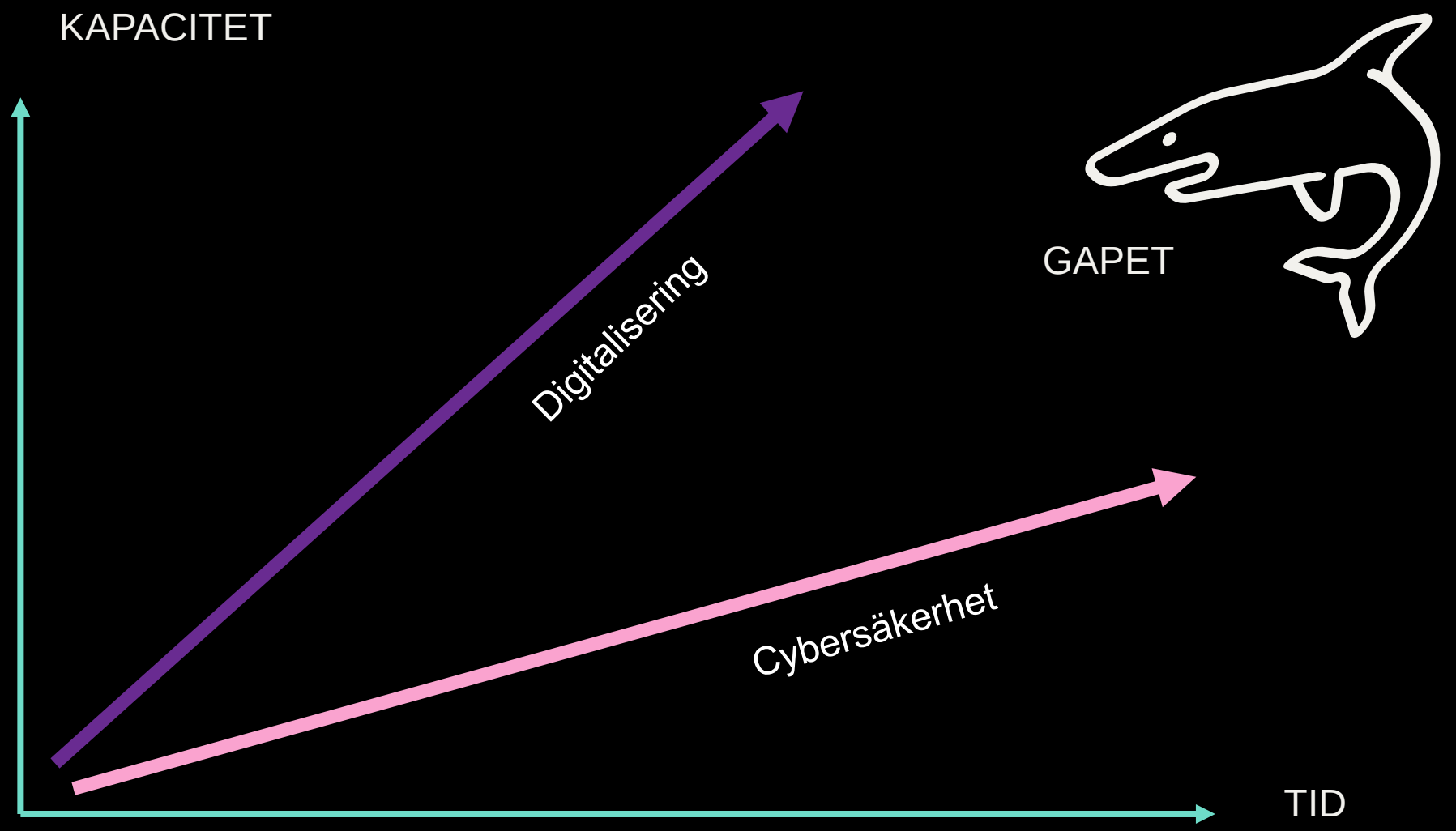
GCI measures the commitment of countries to cybersecurity at a global level, based on five pillars:

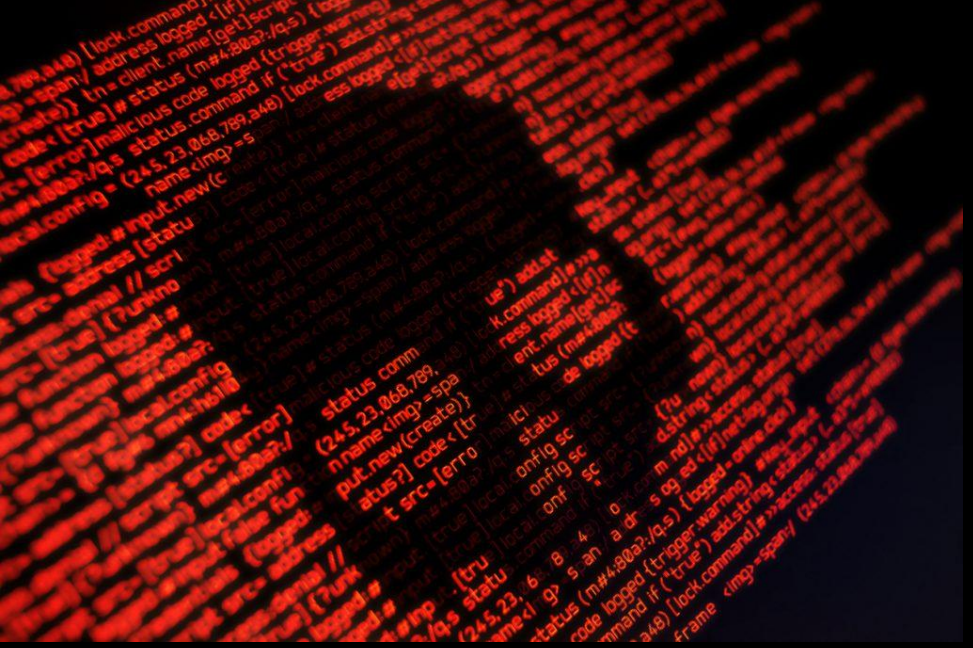
(i) Legal Measures
(ii) Technical Measures
(iii) Organizational Measures
(iv) Capacity Development
(v) Cooperation

Global Cybersecurity Index 2020 (itu.int)

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17
Mauritius	96.89	17

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44
Tunisia	86.23	45
Ireland	85.86	46
Nigeria	84.76	47


KAPACITET
Digitalisering
GAPET
Cybersäkerhet
TID



Läget i Sverige

- I topp när det handlar om att bli utsatta för olika typer av cyberbrott, såsom phishingattacker, BEC-attacker (Business Email Compromise) och supply chain-attacker.

- Svenska anställda bland de minst säkerhetsmedvetna. – Den enskilda individen spelar en central roll i organisationens övergripande cybersäkerhetsskydd, inte minst sett till att 74 procent av alla intrång bygger på någon form av mänsklig komponent.

- Två tredjedelar av svenska anställda inte förstår sin roll och sitt ansvar när det gäller den egna organisationens cybersäkerhet.

- Bland de sämsta när det gäller sånt som att återanvända eller dela lösenord, klicka på okända länkar och lämna ifrån sig inloggningsuppgifter.

Bekräftat: Ransomware-attack mot Svenska kyrkan

Den som besöker Svenska kyrkans externa hemsida möts av information om att det är en pågående driftstörning. Foto: Johan Nilsson/ TT och Fredrik Sandberg/TT

NYHET | PUBLICERAD: 24 NOVEMBER 2023, 11:49 1

44 procent av kommuner och regioner utsatta för cyberattacker

Foto: Adobestock, Mostphotos

Närmare hälften av Sveriges kommuner och regioner har utsatts för it-attacker det senaste året, visar en ny enkät. Ett exempel är förra veckans attack mot 150 kommuners trygghetslarm, som misstänks vara en rysk aktion. För att komma tillrätta med problemen krävs bland annat att offentlig sektor ställer ökade krav på sina leverantörer.

Kalmar kommun utsatt för rysk it-attack

It-attackerna mot svenska verksamheter fortsätter. Kalmar kommun är det senaste offret, och enligt kommunen handlar det om samma ryska grupp som ligger bakom attackerna mot Tietoevry i januari. Händelsen är enligt kommunen polisanmäld.

It-attacken mot Kalix kommun – detta har hänt

UPPDATERAD 25 JANUARI 2022 PUBLICERAD 17 DECEMBER 2021

En hackerattack slog den 16 december ut Kalix kommuns it-system vilket orsakat stora problem i verksamheten och tvingat kommunen att arbeta analogt. Ett omfattande krishanterande arbete sattes in. Det här har hänt hittills.

Coop-anställda hängs ut på darknet efter cyberattack

UPPDATERAD 16 JANUARI 2024 PUBLICERAD 30 DECEMBER 2023

Strax före jul utsattes Coop Värmland för en hackerattack.
Nu har flera anställdas pass och personuppgifter hängts ut på darknet.
– Det här ska vi fixa. Det har vi bestämt oss för, säger Klas Olsson, kommunikationschef på Coop Värmland.

120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade

UPPDATERAD 25 JANUARI 2024 PUBLICERAD 22 JANUARI 2024

Omfattningen av helgens hackerattack växer.
Lönesystemen hos 120 myndigheter är utslagna, flera Regioner och kommuner har problem med sina IT-system och även privata företag har drabbats.

Det är hackergruppen Akira som natten mot lördagen genomförde en cyberattack mot den finska IT-leverantören Tietoevry.

IT-attack mot Munkfors – drygt jobb med återställning

PUBLICERAD 25 SEPTEMBER 2023

Svenska chefer minst oroliga för cyberattacker

Svenska företag drabbas av lika många cyberattacker som danska, finska och norska företag. Trots detta är svenska företagsledare mycket mindre oroliga för attacker än sina nordiska kollegor. Det visar en ny undersökning från Telenor.

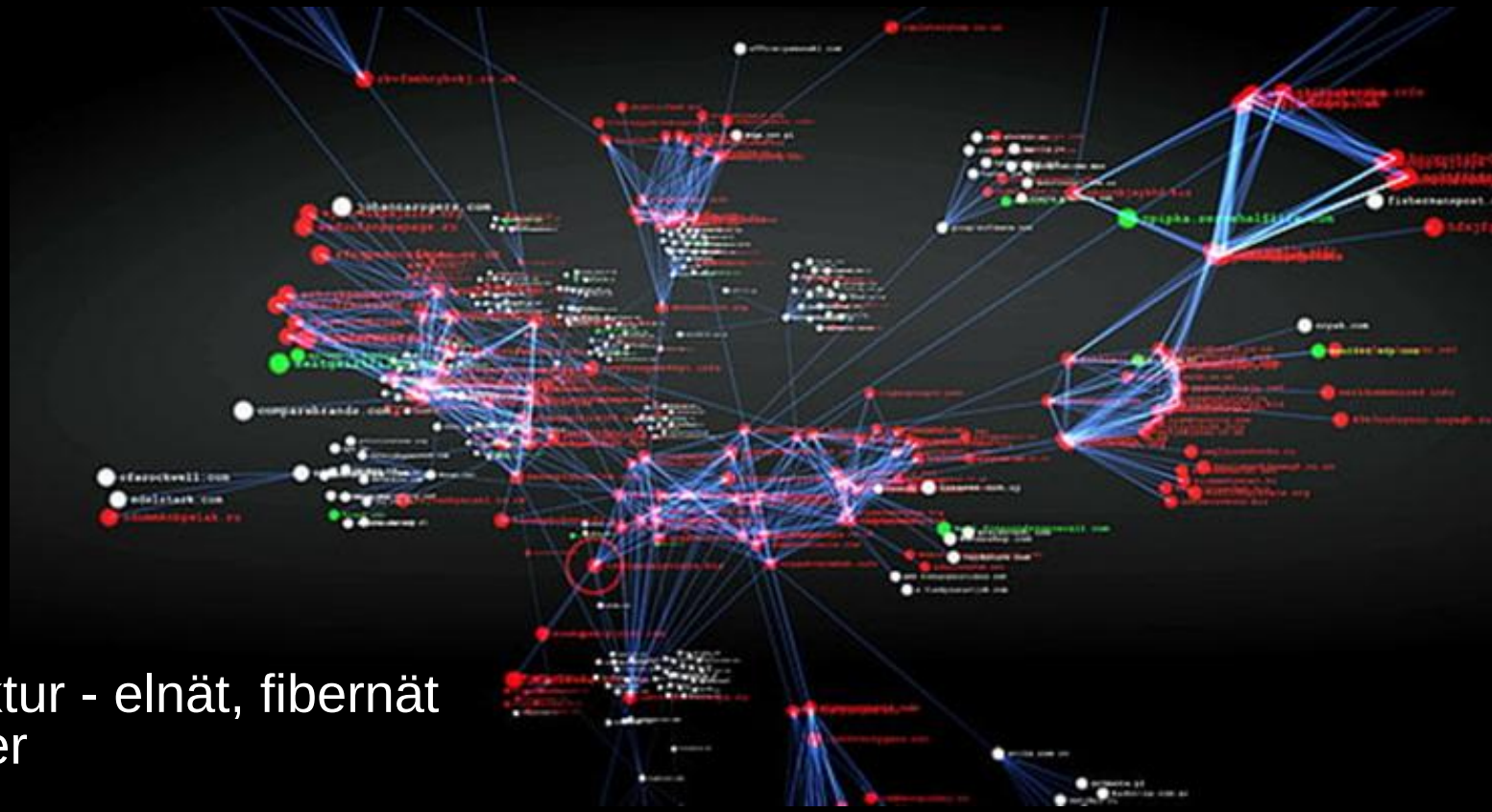
MSB: Sveriges cybersäkerhet på efterkälken jämfört med Ukraina

Foto: Adobestock, Mostphotos

Sveriges offentliga sektor har brister i informations- och cybersäkerhetsarbetet, enligt MSB:s nya årsrapport. För att råda bot på detta vill myndigheten att Sverige utreder sin digitala suveränitet, utvecklar egna molnliknande lösningar och förändrar eller instiftar nya lagar på säkerhetsområdet.

Varför är det så här?

Utmaningar



- Kompetensförsörjning
- Nya utbildningar
- Redundans i digital infrastruktur - elnät, fibernät och trådlösa kommunikationer
- Nya innovationer
- Nya företag
- Säkra arbetsplatser
- Medvetenhet och förståelse – det är människor det hänger på!

Kompetensbehov

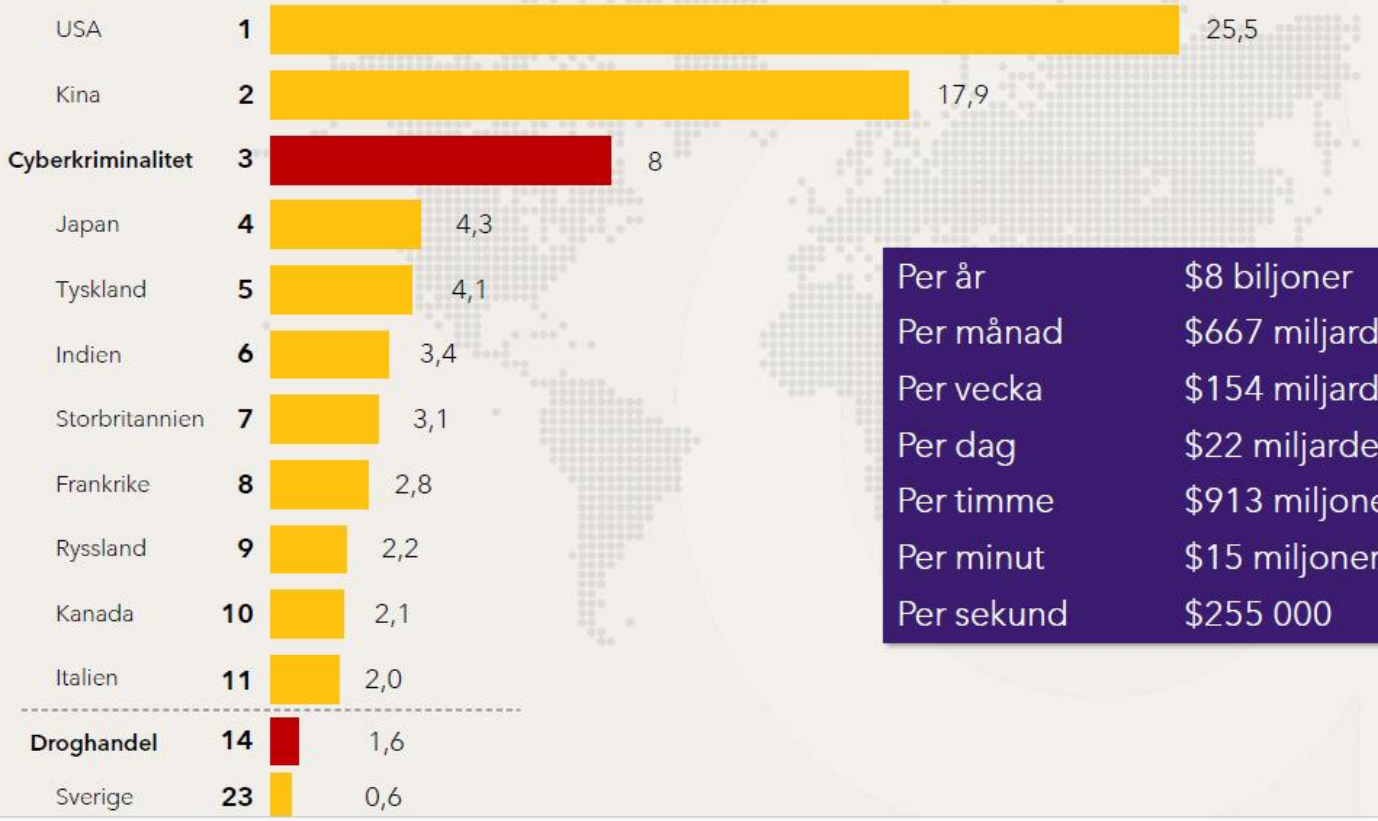
Den globala cybersäkerhetsarbetsstyrkan är på en rekordnivå, med 4,7 miljoner yrkesverksamma.

464 000 fler cybersäkerhetsproffs har tillkommit under 2023, men 3,4 miljoner fler cybersäkerhetsarbetare behövs

Om våra digitala infrastrukturer inte är säkra riskerar vi våra samhällskritiska funktioner.

Vad är det som händer och varför?

Topp 10 största ekonomier i världen 2022 (biljoner USD)



Per år	$8 biljoner
Per månad	$667 miljarder
Per vecka	$154 miljarder
Per dag	$22 miljarder
Per timme	$913 miljoner
Per minut	$15 miljoner
Per sekund	$255 000


Hacktivister
Script kiddos
Cyberkriminell verksamhet
Statligt sponsrade aktörer
Insider

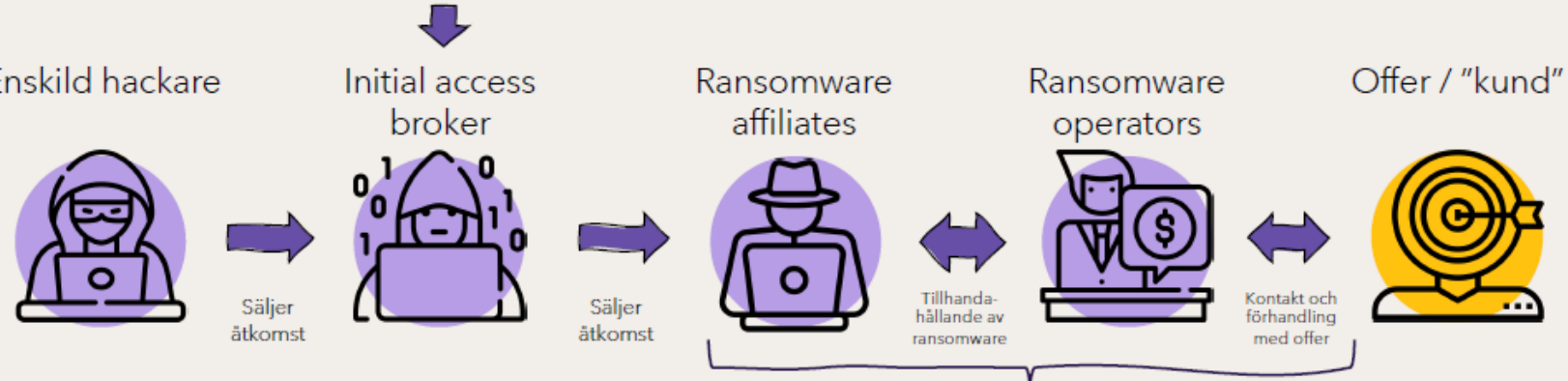
dizparc

Hackekonomin

- Cyberkriminellas kapacitet

Automatiserade verktyg

Riktar in sig på att hitta kända sårbarheter i populära applikationer för att enkelt få initial åtkomst



500-1.500 kr

5.000-100.000 kr

Ransom på 100.000 till >10.000.000 kr

Mål
Hitta lätta offer exponerade på internet. Typiskt sårbara fjärrskrivbord, VPN osv. utan multifaktorsautentisering.

Styrkor
Stor kapacitet, dvs. många till antalet.

Svagheter
Begränsad kompetens.
Låg uthållighet i angreppsförsök.

Mål
Förädla, eller "vattna åtkomsten" genom eskalering av rättigheter i målmiljön.

Styrkor
Högre kompetens och uthållighet.

Svagheter
Färre resurser/kapacitet.

Mål
Skaffa de sista nödvändiga åtkomsterna och sedan sprida ransomware i miljön.

Styrkor
Hög kompetens och uthållighet.

Svagheter
Begränsad kapacitet.
Arbetar endast med miljöer med hög åtkomstgrad.

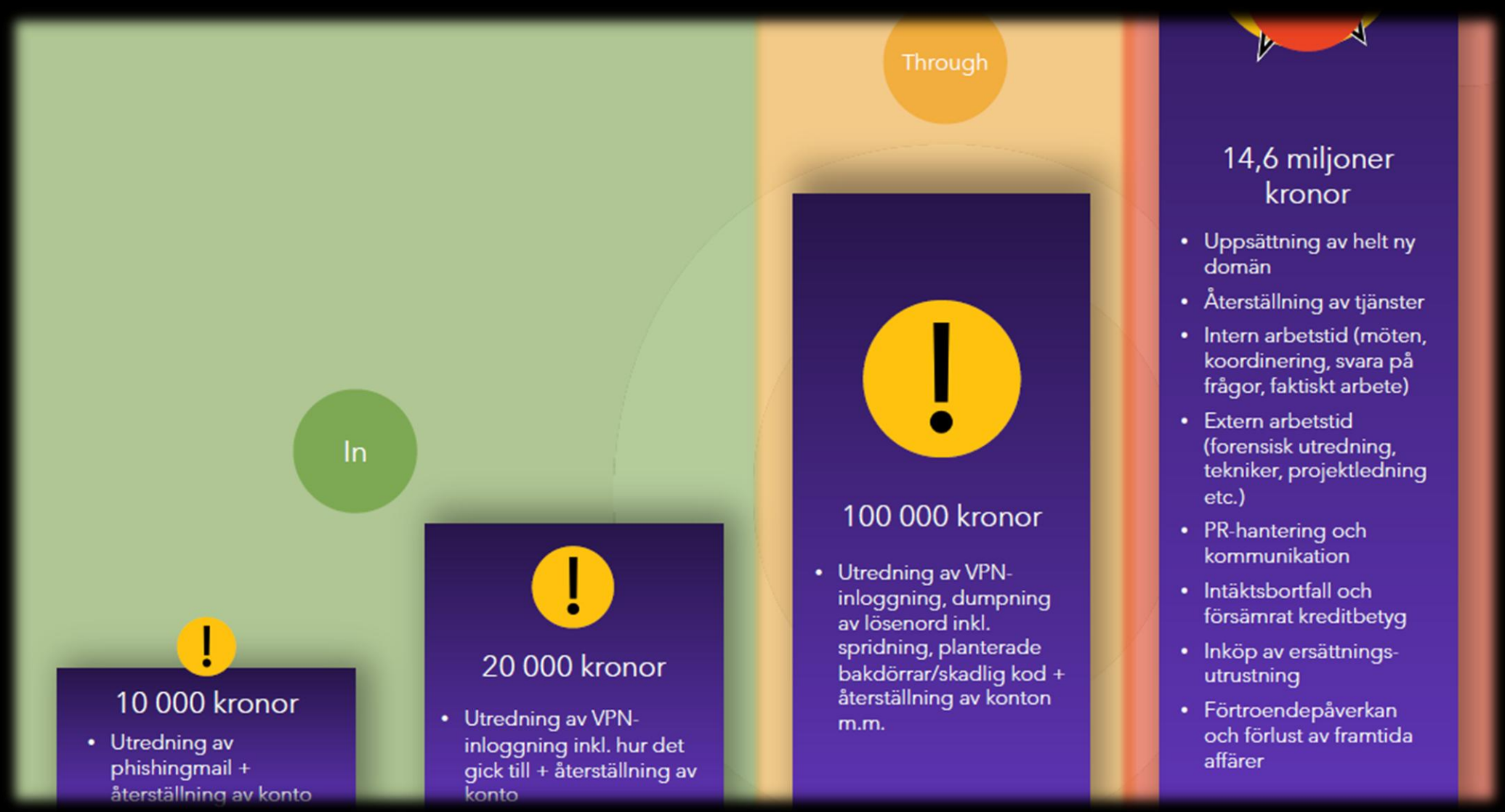
Mål
Tillhandahålla "ransomware-as-a-service", förhandla med offer och ta % av lösensumma.

Styrkor
Specialiserade på utveckling av ransomware/kryptovirus samt förhandling med offer

Svagheter
Begränsad kapacitet.
Arbetar endast med miljöer

Att drabbas av en cyberattack blir också allt mer kostsamt.

Under 2023 fördubblades den genomsnittliga kostnaden från en cyberattack-relaterad händelse till i genomsnitt **14,6 miljoner** kronor, från 6,8 miljoner år 2022.


In
Through
10 000 kronor
• Utredning av phishingmail + återställning av konto
20 000 kronor
• Utredning av VPN-inloggning inkl. hur det gick till + återställning av konto
100 000 kronor
• Utredning av VPN-inloggning, dumpning av lösenord inkl. spridning, planterade bakdörrar/skadlig kod + återställning av konton m.m.
14,6 miljoner kronor
• Uppsättning av helt ny domän
• Återställning av tjänster
• Intern arbetstid (möten, koordinering, svara på frågor, faktiskt arbete)
• Extern arbetstid (forensisk utredning, tekniker, projektledning etc.)
• PR-hantering och kommunikation
• Intäktsbortfall och försämrat kreditbetyg
• Inköp av ersättnings-utrustning
• Förtroendepåverkan och förlust av framtida affärer

Fallet Vastaamo – skräckexemplet som blev verklighet

- 2020 utsattes finska psykoterapi-koncernen Vastaamo för en omfattande cyberattack
- Journaler från ca 36 000 patienter samt information om 400 medarbetare läckte
- Vastaamo krävdes på 40 Bitcoins i ransom (ca €450 000 vid tillfället)
- När inte detta betalades utpressades istället ca 30 000 patienter via e-post för att enskilda persondata inte skulle släppas publikt
- Vastaamo försattes i konkurs februari 2021
- Ex-CEO dömdes till 3 månaders villkorlig dom för GDPR-brott

Vi är redan i krig

Hybridhoten ökar,
kan exempelvis vara
fysiskt sabotage mot
infrastruktur,
påverkanskampanjer
och cyberattacker.

Vem har ansvar?

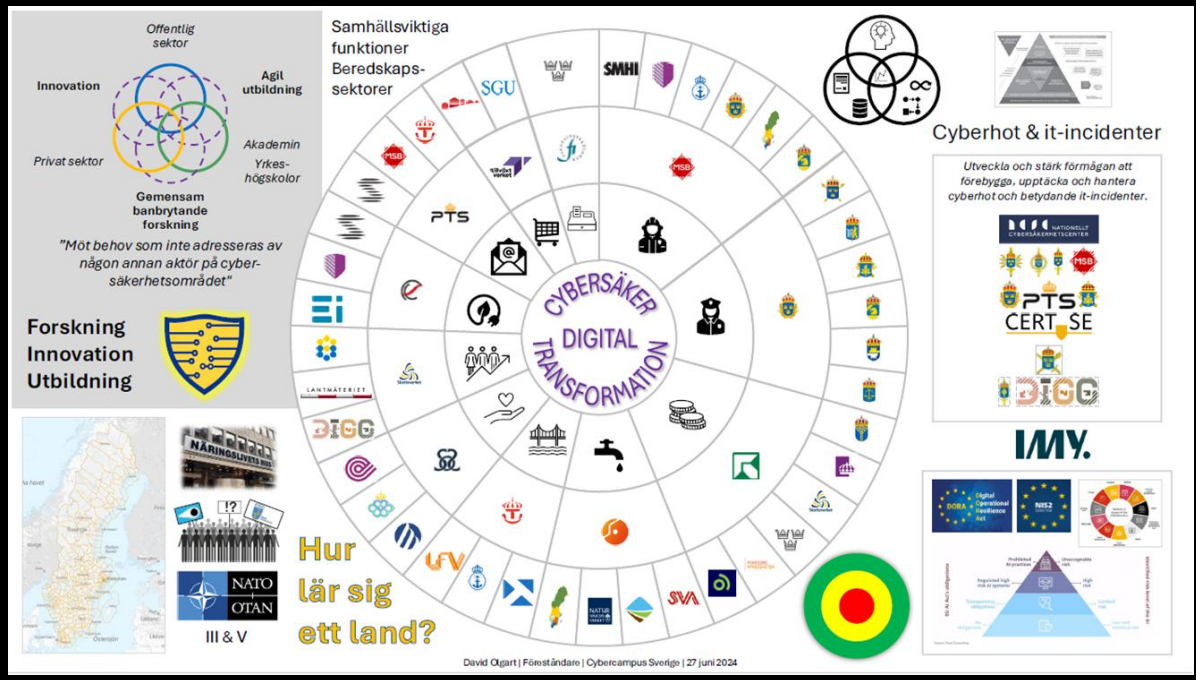
Nya krav och direktiv

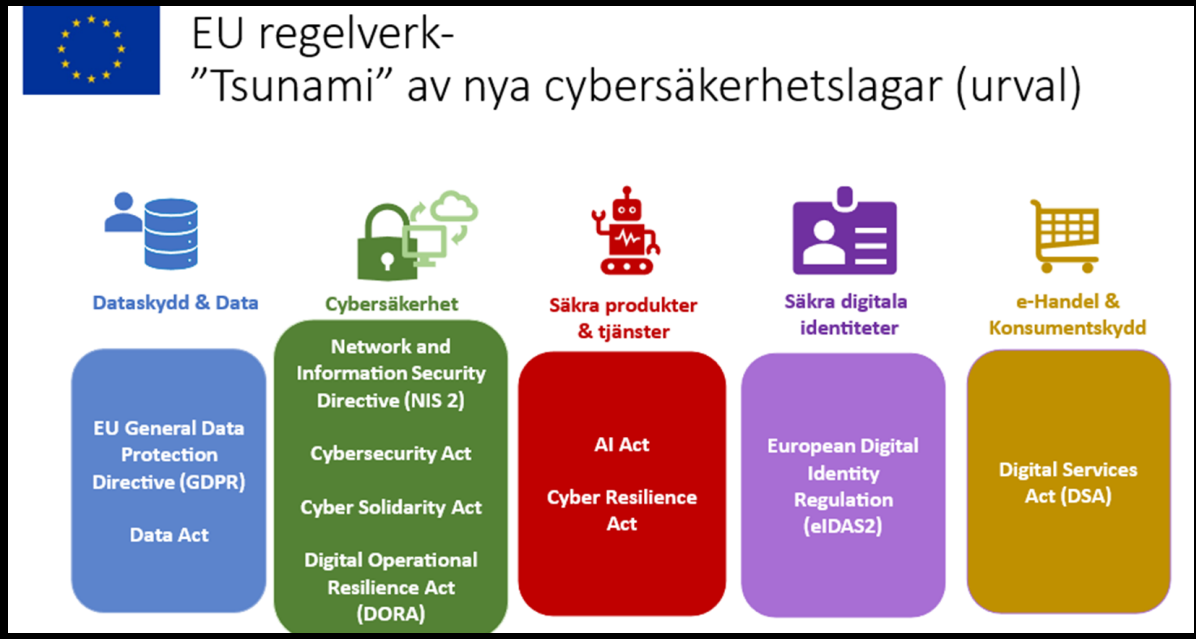
- NIS2-direktivet
- CER kompatibelt
- ISO27001
- CIS Controls
- NIST

Sanktioner

Tillsynsmyndigheterna får besluta om sanktionsavgifter vid överträdelser av Cybersäkerhetslagen. Den maximala avgiften blir det högsta av:

1. **2 %** av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. **10 miljoner Euro**.





Vem ska göra jobbet?

-”Varje verksamhetsutövare behöver ta situationen på allvar!”

Carl-Oskar Bohlin, Minister för civilt försvar

- Styrelse- och ledningsfråga. Måste drivas uppifrån.
- Säkerhetschefens roll har förändrats. Säkerhet måste ägas av hela verksamheten och förstå affären.

Vad vi gör då?

Skydda din information

- Installera säkerhetsuppdateringar på din telefon, dator och andra enheter så fort det är möjligt.
- Använd tjänster med tillförlitlig kryptering för samtal och meddelandeöverföring, det finns flera sådana, ett par exempel är tjänsterna ”Signal” och ”Cryptify”. Hör gärna med PTS, Post- och telestyrelsen, om du behöver för ytterligare vägledning.
- Var vaksam mot försök till nätfiske och försök att plantera skadlig kod, till exempel via webbsidor eller länkar i e-mejl eller sms.
- Skydda din e-legitimation – logga aldrig in på uppmaning av någon annan.

Källa: MSB

Tips för att undvika dataintrång

- Ha starka och unika lösenord för varje konto, gärna i form av lösenordsfraser.
- Dela aldrig privata uppgifter med någon annan.
- Godkänn inte vänförfrågningar från okända personer utan att först verifiera deras identitet.
- Logga ut från sociala medier när du inte använder dem.
- Var kritisk till meddelanden från ”vänner,” särskilt när det handlar om ekonomiska förfrågningar.

Källa: Stöldskyddsföreningen

5 sätt att preppa

- Avregistrera gamla och oanvända konton och appar som du inte längre använder.
- Säkra inloggningar. Använd lösenordshanterare som krypterar dina lösenord och använd tvåfaktorsautentisering. (inte samma lösenord överallt)
- Uppdatera din enheter.
- Säkerhetskopiera viktiga filer. Föröver viktiga dokument till molntjänst, en USB sticka eller skriv ut dem och förvara på säkert ställe.
- Fysisk telefonbok. Viktiga telefonnummer som du kan behöva nå när din telefon är hackad eller om den slutar fungera helt.

Phising, ett stort problem.
1 av 3 klickar

- Skapa förståelse och var förstående.
- Det är människors beteende som vi skall förändra, vi skall inte konfigurera ett system.
- Vi måste ha respekt för att beteenden tar tid att ändra på
- Viktigt att anpassa till er egen företagskultur och de arbetssätt som finns etablerade idag, och vissa saker kanske också måste utmanas!
- Målet är att skapa engagemang

Cyberförsäkring

- Allt mer populära men kraven för att teckna ökar.
- Behöver visa upp starka it-säkerhetslösningar, välutbildade medarbetare och ordentliga krisplaner.
- De två mest förekommande kraven för att få teckna en cyberförsäkring är flerfaktorautentisering och aktiv säkerhetsövervakning och incidenthantering (MDR, Managed Detection and Response).

Incident Respons-strategi

- Förberedelser: steg för att öka motståndskraft
- Upptäckt och analys: Identifiera och analysera incidenter
- Avgränsning, utrotning och återställning: steg för att adressera incidenten
- Kommunikation: Informationsspridning och PR-relaterad kommunikation. Internt och externt.
- Post-incident-aktiviteter: Analys, rapportering, lessons learned

Företaget interna resurser

IT-partner IT-resurser

Säkerhet övervakning

Fler?
Forensik
Juridik
PR

Tänk ISO, skyddsrond eller arbetsmiljögenomgång

- Vilka roller behöver involveras?
- Vilka befogenheter har de roller som är involverade?
- Matris för allvarlighetsgrad och eskaleringspunkter.
- Kommunikationsplan.
- Dokumentation och strukturkapital (mallar) vid incidenthantering som säkerställer effektivitet och kvalitet och konsekventa utfall i incidenthanteringsarbetet.
- Utbildning och övning.
- Utbildning och övning.
- Utbildning och övning.

Se till att ha alla planer i en pärm eller separat lättåtkomlig hårddisk eller usb!

Vilka är våra mest kritiska tillgångar och resurser?

Att förstå vad som är mest kritiskt och vilken påverkan störningar på kritiska resurser kan få är viktigt för att kunna definiera en effektiv plan. Syftet är att kritiska delar skall prioriteras först vid en incident.

Utifrån verksamhetsperspektivet

Produktionsverksamhet
Tekniker/fältarbetare
Lager och logistik
Forskning och utveckling
Konfidentiell information
Kundregister (GDPR)
Etc.

Utifrån IT-perspektivet

IT-infrastruktur
Affärssystem
Filytor och lagring
Samarbetsplattform
Webshop
Etc.

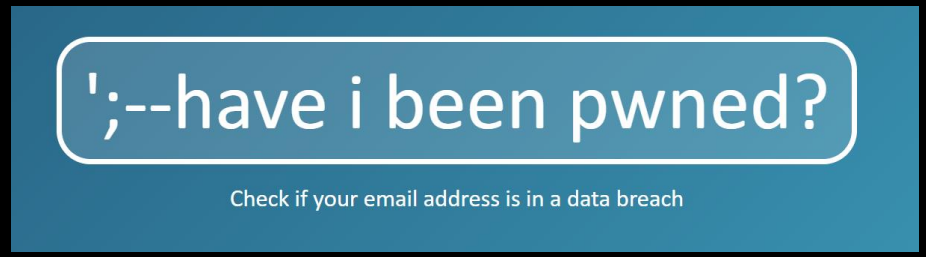
Myndigheten för samhällsskydd och beredskap

https://MSB.se
https://cert.se

Utlysningar om finansiering.

Cyberlyftet - En introduktion till cybersäkerhet | RISE

Denna kurs ger en grundläggande förståelse för hur du skyddar digitala system, nätverk och data mot cyberhot. Genom ett antal kapitel och praktiska övningar kommer du att lära dig att identifiera och hantera olika cyberhot.



https://haveibeenpwned.com

Vänta inte.
Var smart.
Ta hjälp.
Var förberedd.
Träna!

Skydda din egendom!

Ingrid Ivars
Innovation Manager
+46 768 36 68 68
Ingrid.ivars@compare.se

Stiftelsen Compare Karlstad
www.compare.se