



Cybersikkerhet 2025

13th
Annual
Edition

Trusselbilde, utfordringer og anbefalinger

THE STATE OF CYBER SECURITY 2025

Top threats, emerging trends, and CISO recommendations



01 INTRODUCTION

02 2024 CYBER SECURITY EVENTS

03 CYBER SECURITY TRENDS

- Cyber Wars - 2024 Edition
- The Ransomware Ecosystem
- The Rise of Infostealers
- Cloud Complexities

INTRODUCTION

I'm happy to introduce the 13th annual edition of Check Point's State of Cyber Security. 2024's advancements like AI and cloud infrastructure improved our daily lives but also benefited cyber criminals. This report highlights the real-world impact of these changes, offering 2025 insights and recommendations from and for CISOs.

With over a decade of analysis, Check Point Research insights come from unparalleled data sources that no other company combines. We gather attack telemetry from networks, cloud, email, endpoints, and mobile devices across enterprise and SMB customers. By incorporating incident response, dark web, and open-source findings, we achieve visibility in over 170 countries to reveal global and regional trends.

The 2025 State of Cyber Security report highlights key threats, including:

- The AI tactics that swayed a third of global elections through disinformation.
- A 58% surge in infostealer attacks, focusing on corporate access.

Cyber Security Trends 2025

Cyber Wars

Nation-states are leveraging AI-driven tactics, including disinformation campaigns and disruptive malware, to weaken systems and sow chaos globally.

Ransomware

Criminals are shifting from data encryption to extortion, with ransomware emerging as one of the most significant cyber threats to businesses worldwide in 2024.

Infostealers

These malware attacks have surged by 58%, stealing credentials and sensitive data, impacting individuals and organizations alike.

Cyber Security Stats

3.5K+

Weekly Attacks on the Education Sector

10%

Of Ransomware Victims are Healthcare

58%

Increase in Infostealer Attempts in 2024

\$200K

Median Ransom Payment in 2024



Last ned hele rapporten her



**THE STATE OF CYBER
SECURITY 2025**

00

Trender for 2025

1

Cyberkrig

4

Endepunkter

2

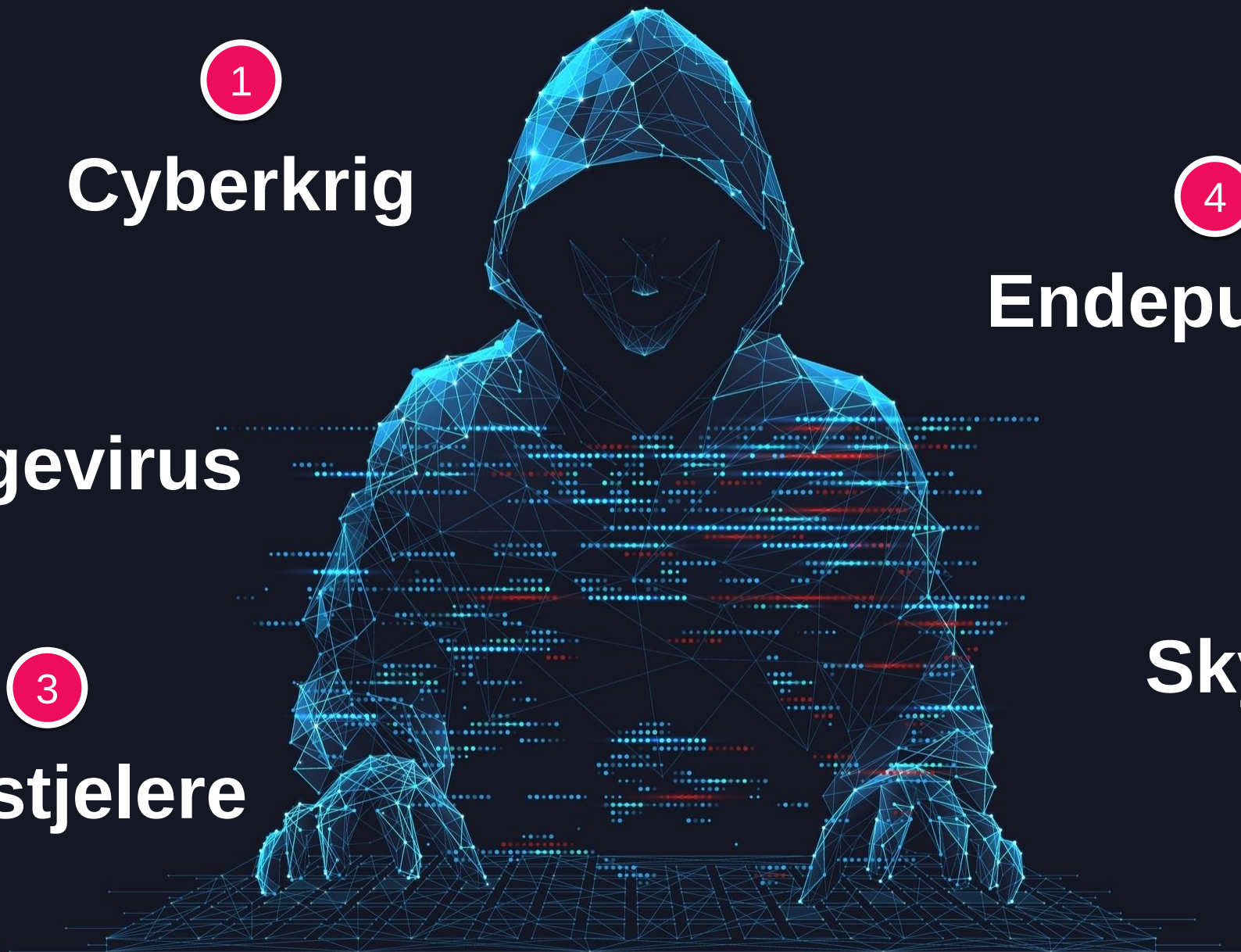
Løsepengevirus

3

Infostjelere

5

Skytjenester



Hovedpunkter fra trusselrapporten

- **Cyberkrigføring** – Statlige aktører utfører langvarige angrep i stedet for korte.
- **Løsepengevirus** fokuserer mer på utpressing gjennom dataeksfiltrering enn kryptering.
- **58%** økning i **Infostealer-angrep** årlig. Fokuserer på å stjele tokens og identitet fra BYOD-enheter.
- **AI** øker desinformasjons- og påvirkningskampanjer innen valg og offentlig opinion.
- Kompromitterte **endepunkter** utnyttes som en viktig angrepsvektor mot bedriftsnettverk.
- **Hybride nettverk** muliggjør toveis lateral bevegelse mellom lokale systemer og skyen.



- Sektorer innen sensitive **teknologiske forsyningskjeder** opplever den største økningen i angrep per organisasjon.
- 1 av 25 **angrep** i 2024 brukte en sårbarhet som ble offentliggjort i 2024.
- **Utdanning** har vært den mest utsatte sektoren i fem år på rad, med en **økning** på **75%** årlig. Cyberkriminelle retter seg mot mål som vanligvis har svakere sikkerhet.
- **Helsevesenet** blir den nest mest utsatte sektoren for løsepengevirus, noe som viser at trusselaktører ikke har noen moralske grenser.

01

Trussel Typer & Løsninger

Hovedpunkter for trussel

Foreslått løsning



Cyber Krig

Fokus på å undergrave offentlig tillit, utnytte splittelser i samfunnet og destabilisere institusjoner:

- Desinformasjon og påvirkningskampanjer
- Statstilknyttet Hacktivism
- Destruktiv og ny, avansert skadevare

Lag-på-lag sikkerhet,
 gjerne i felles
 plattform

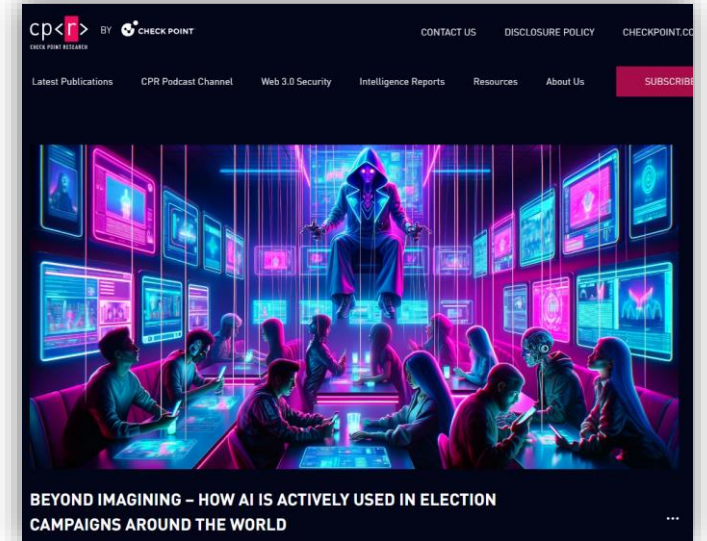
Statlige aktører utfører angrep over tid (kroniske) vs akutte

Desinformasjon og påvirkningskampanjer

- Valgrelaterte kampanjer som påvirkes
- Benytter AI for å lage innhold
- Hold deg oppdatert på research.checkpoint.com



Operation MiddleFloor: Disinformation campaign targets Moldova ahead of presidential elections

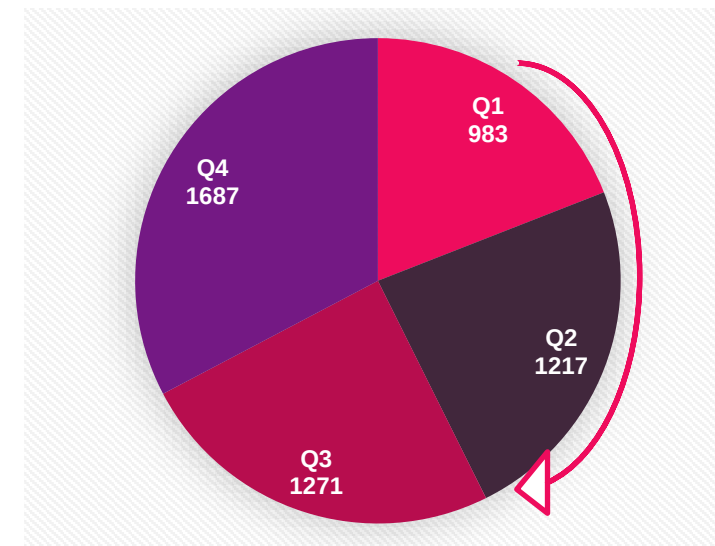
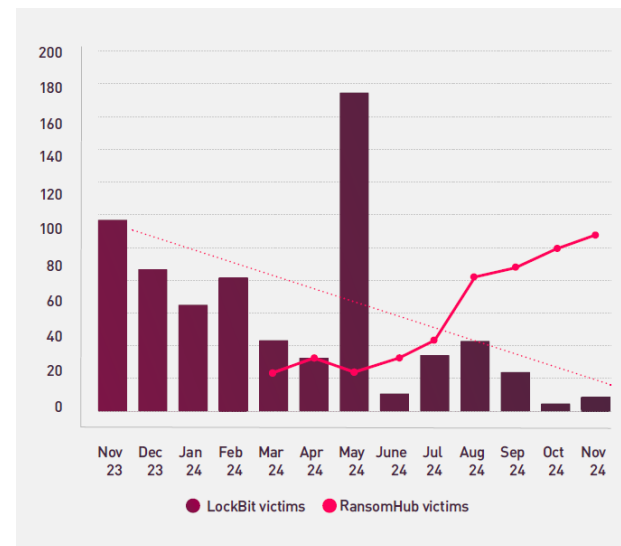


How AI is Actively Used in Election Campaigns Around the World

AI brukes flittig for å spre desinformasjon og påvirke valgkampanjer og folks meninger generelt

Løsepengevirus – Politiaksjoner påvirker miljøet

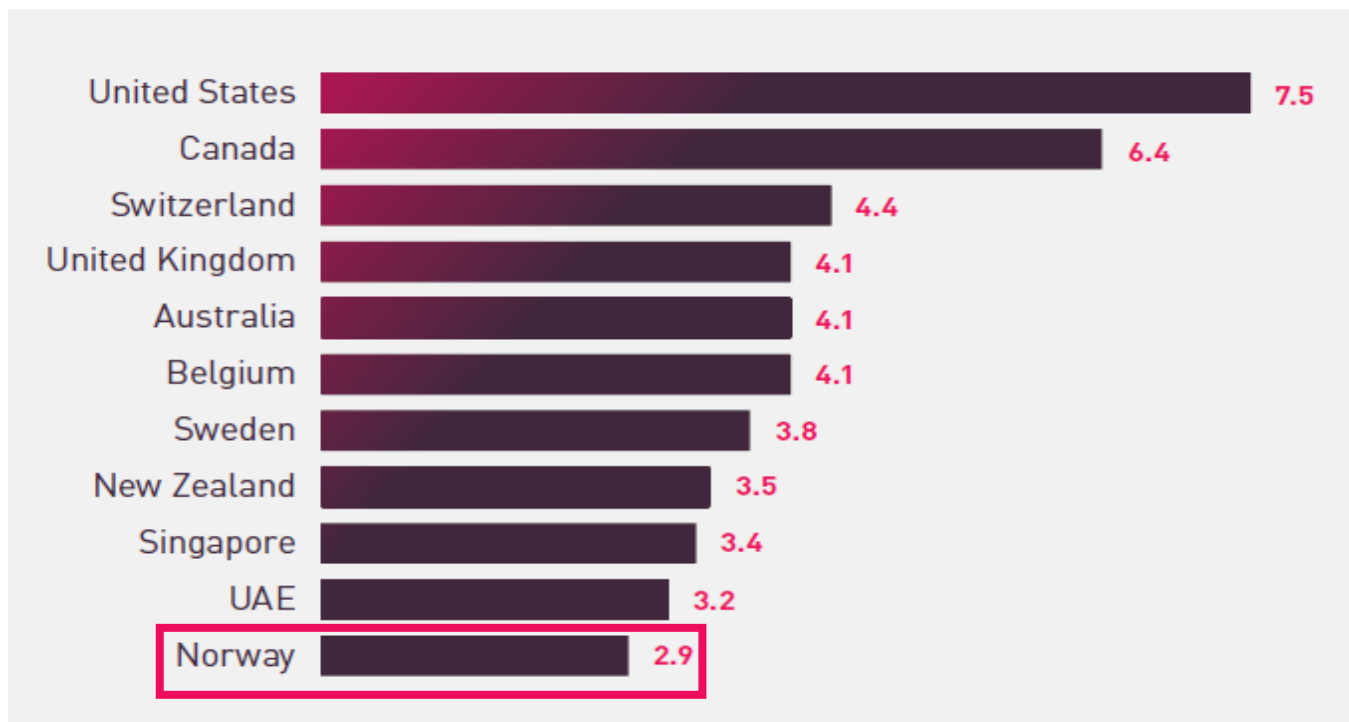
- Lockbit og ALPHV tas ned
- RansomHub etableres
- Aktørene er raskt oppe igjen etter politiaksjonene
- Økosystemet er fragmentert



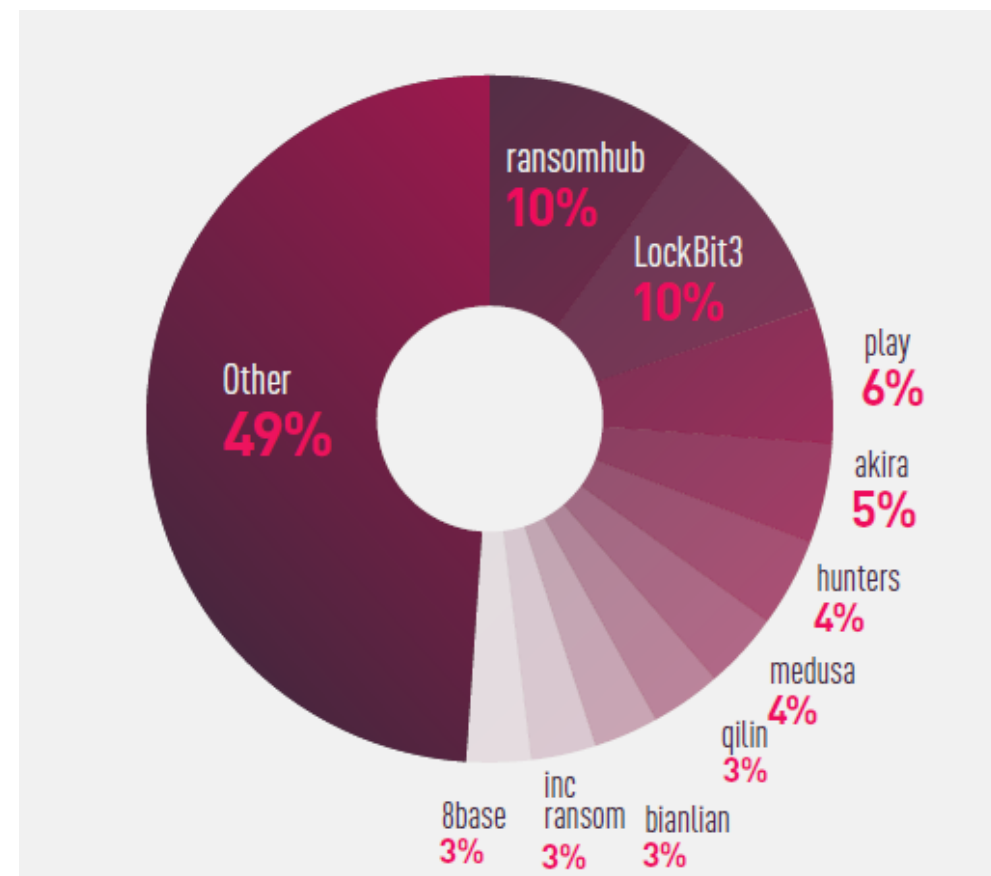
Løsepengevirus fokuserer på utpressing gjennom data-lekkasje fremfor kryptering

Løsepengevirus – Hvem er skadelidende?

- Data fra 5,200 organisasjoner som ikke betalte er postet på Dark Web av over 95 ulike grupperinger
- 50% av de berørte selskapene er i USA



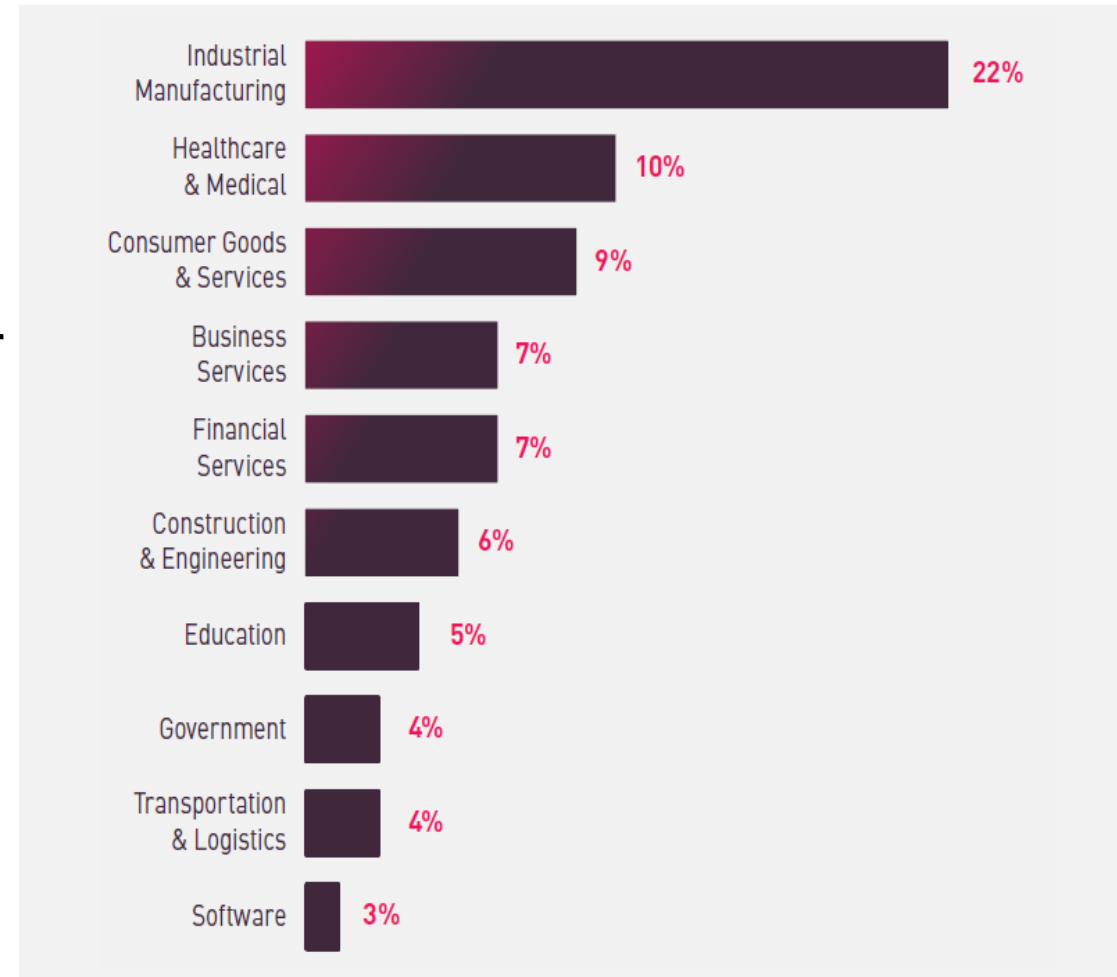
Ofre pr 1 Million innbyggere



Løsepengevirus - Helsevesen

- **Fokuserte angrep mot helsevesen**
 - Den “nest mest” angrepne sektoren
 - Over **65%** of skadelidende innen helse er basert i USA

Endepunkt sikkerhet



Helsevesenet er den nest mest utsatte sektoren for løsepengeangrep, noe som viser at trusselaktører ikke har noen moralske grenser

Infostjeler – Hva er det?

Nettleser Data

Identitet

Betalingskort

Informasjonskapsler

Crypto lommebøker

Skjermbilder

Filer



58 % økning i Infostealer-infeksjoner årlig, med fokus på å stjele tokens og identitet fra BYOD-enheter.

Infostjelere

- **“Spray & Pray” strategi**
 - Mer enn **70%** av infiserte maskiner er ikke tilknyttet bedriften (non corporate)
- Er et nøkkelverktøy for Initial access brokers (IABs)



Endepunkt sikkerhet

SASE

Endepunkter & ORBs i 2025

- **Masseutnyttelse av endepunkter**
 - Brannmurer
 - IOT enheter
 - SOHO rutere
- **Blir en del av**
 - Angripernes infrastruktur og angrepsvektor



Velg produsent med
få sårbarheter

IoT/OT beskyttelse

Kompromitterte endepunkter brukes til å lage **Operational Relay Boxes (ORB-er)**, som anonymiserer og videresender kommunikasjon. Dette gjør at enheter uvitende blir mobilisert som "soldater" på cyberkrigsfeltet.

Sky

- Enorm kompleksitet fører til feilkonfigurasjoner
- Hybride miljø muliggjør lateral bevegelse
- SSO kontoer angripes gjennom IDP tilbyder
- Store språkmodeller i sky infiseres

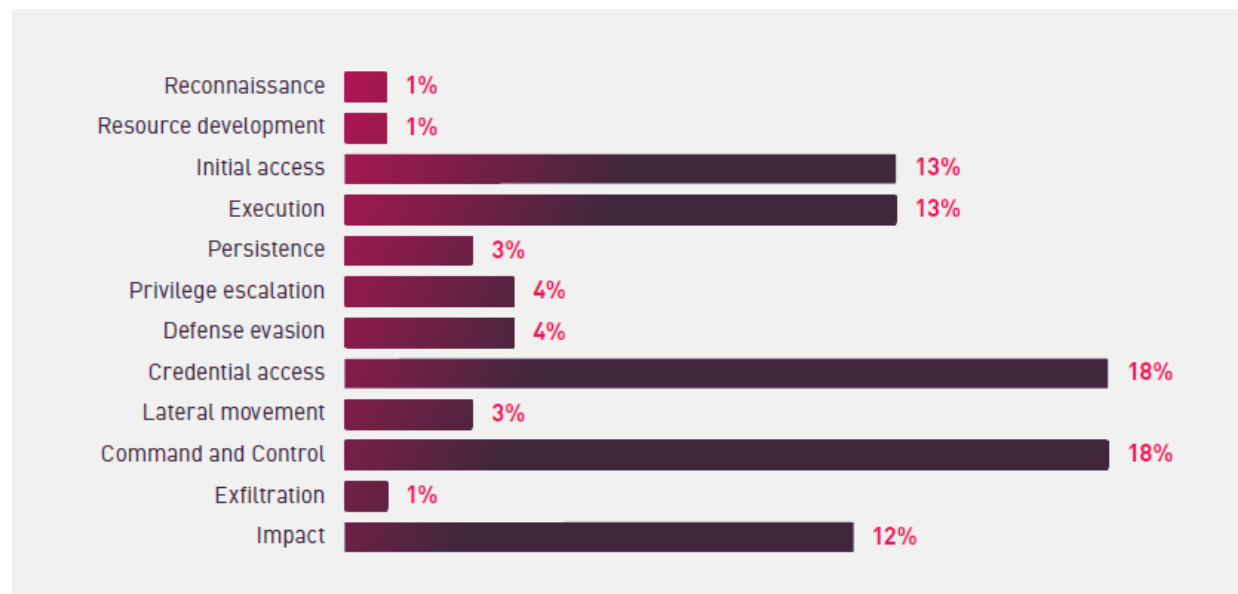
Posture Management
Workload Protection

SaaS overvåking



Ceek Point IRT – Hva har vi lært?

- Angrep oppdages ofte sent i angrepssyklusen:
 - Ved bruk av identitet (18%)
 - Ved kommunikasjon med C&C servere (18%)
- I kun 12% av tilfellene ble angrep oppdaget i påvirkningsfasen!



Ulike angrep som utløser respons, basert på logger

Lag-på-lag sikkerhet,
 gjerne i felles
 plattform

02

Trussel statistikk

Toppliste Skadevare

- **FakeUpdates** - Er en nedlaster som distribueres gjennom websider
- **AgentTesla** – avansert Remote Access Trojan (RAT) og infostealer.

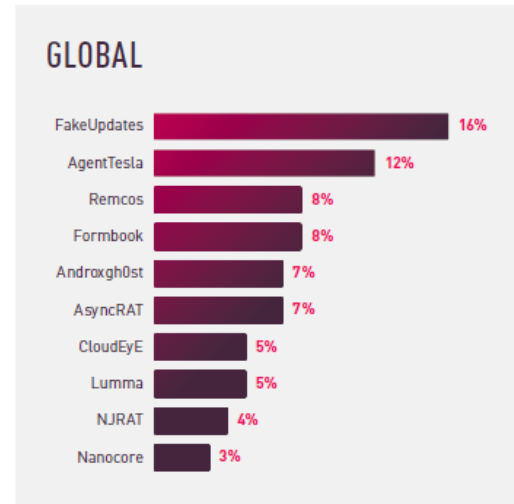


Figure 8 - Most prevalent malware globally - 2024.

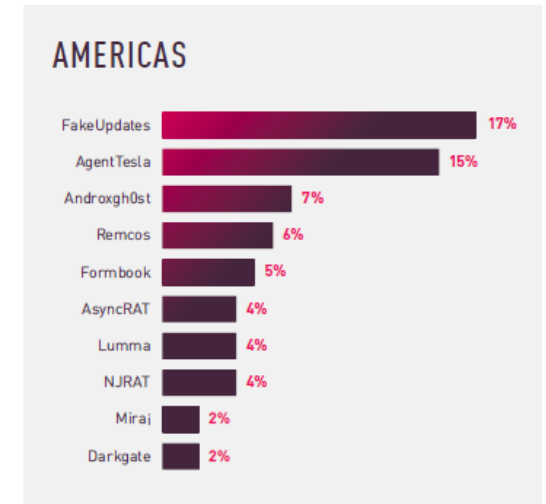


Figure 9 - Most prevalent malware in the Americas - 2024.

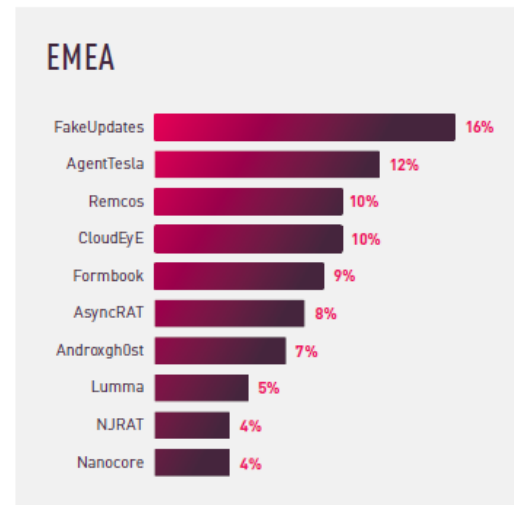


Figure 10 - Most prevalent malware in EMEA - 2024.

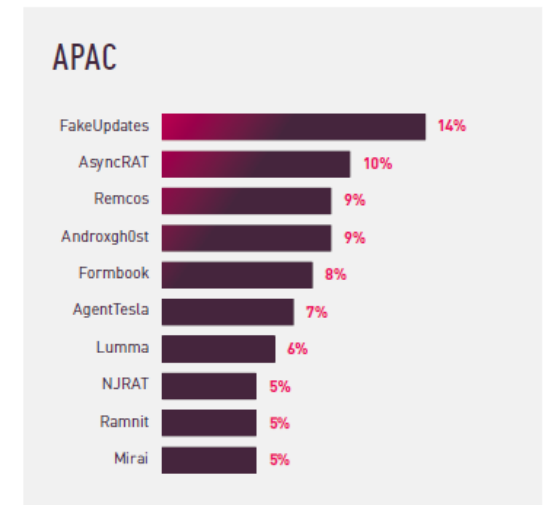
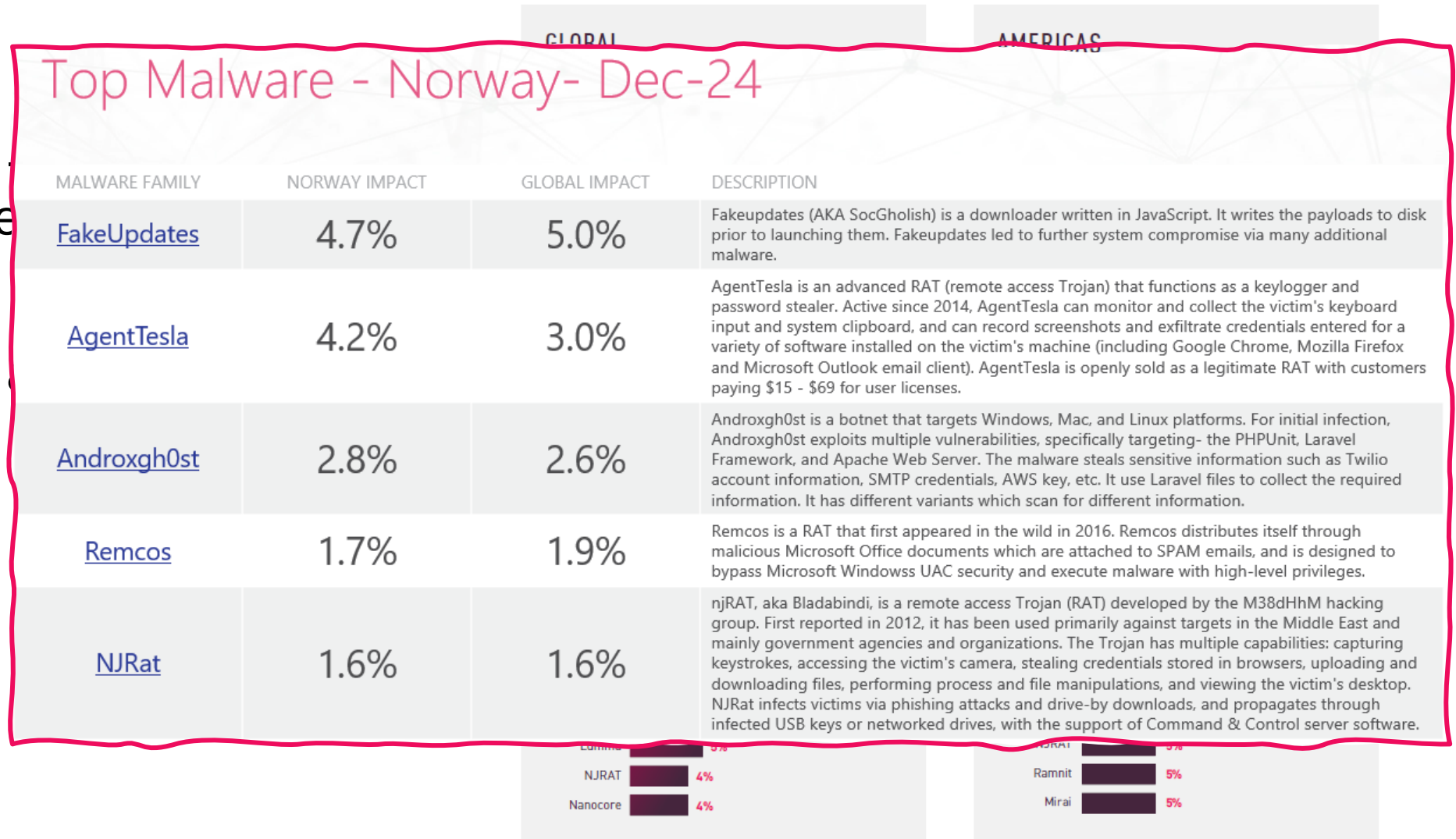


Figure 11 - Most prevalent malware in APAC - 2024.

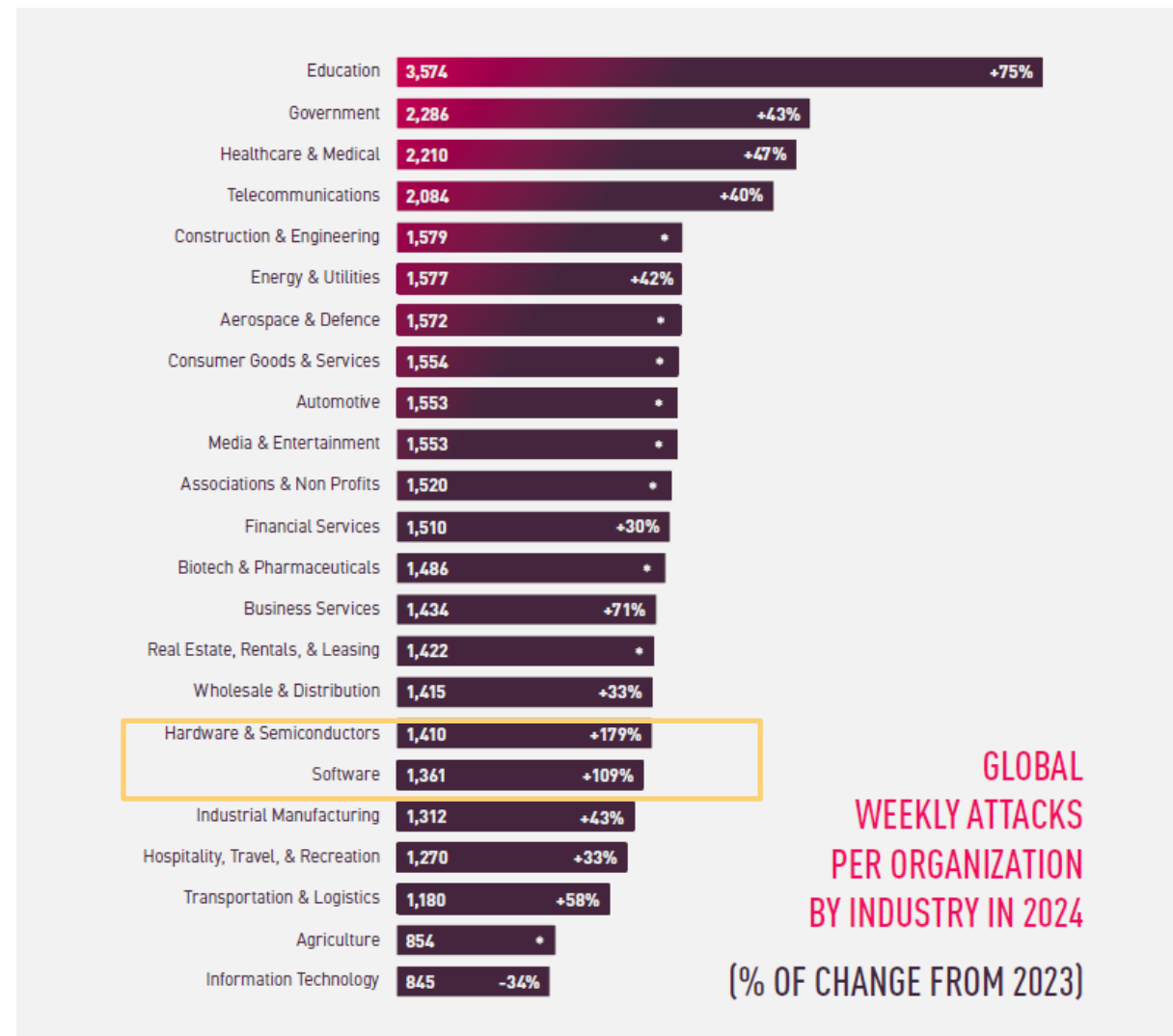
Topliste Skadevare

- **FakeUpdates** – distribueres gjennom
- **AgentTesla** – Access Trojan



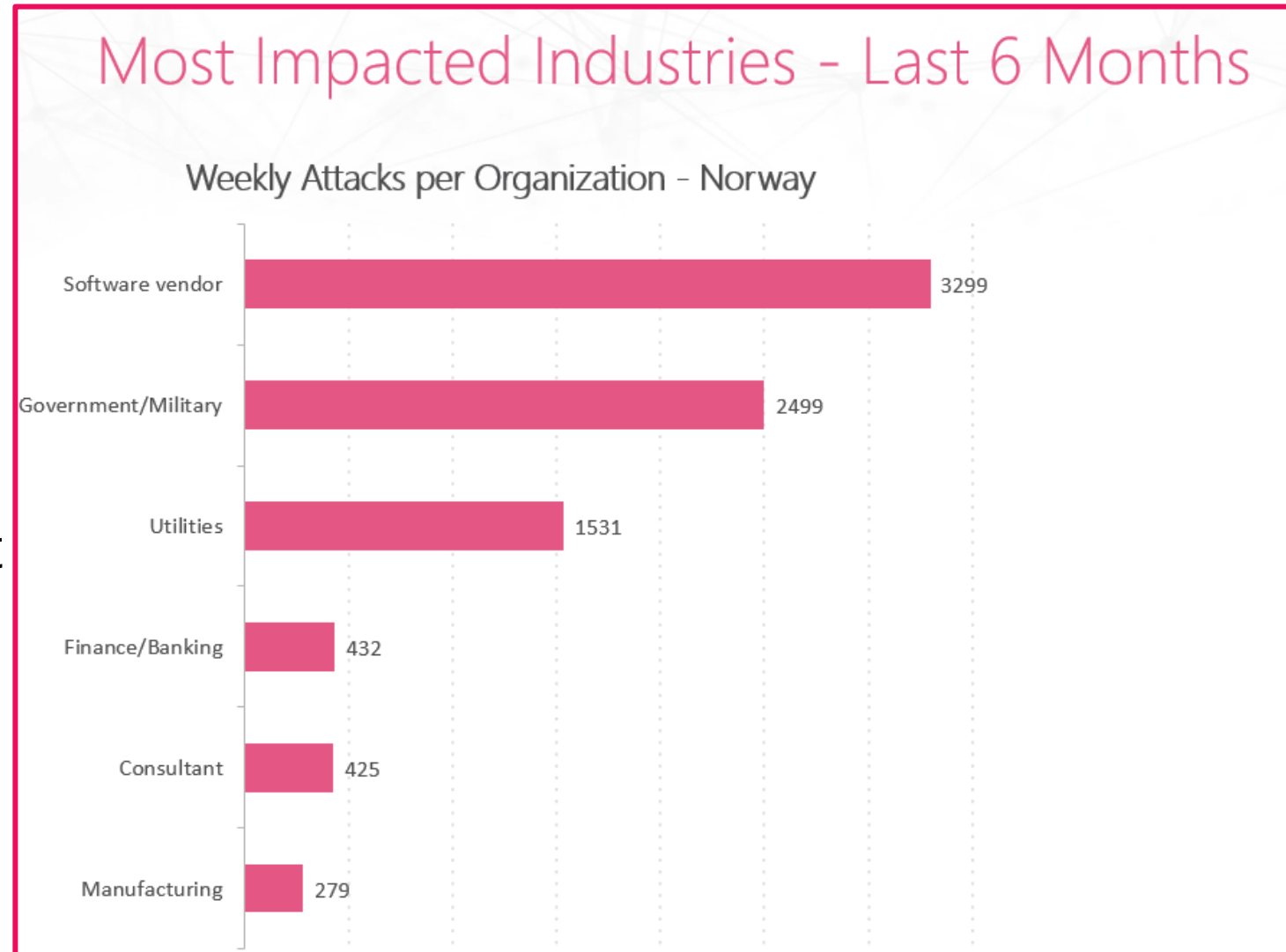
Ukentlige angrep per organisasjon / sektor

- Utdanning er mest utsatt
 - Ofte et enkelt mål pga lavere sikkerhet
 - **75% årlig økning i angrep**
- Teknologi sektoren har hatt størst økning av angrep
 - **Maskinvare & Halvledere** + 179%
 - **Programvare** + 109%



Ukentlige angrep per organisasjon / sektor

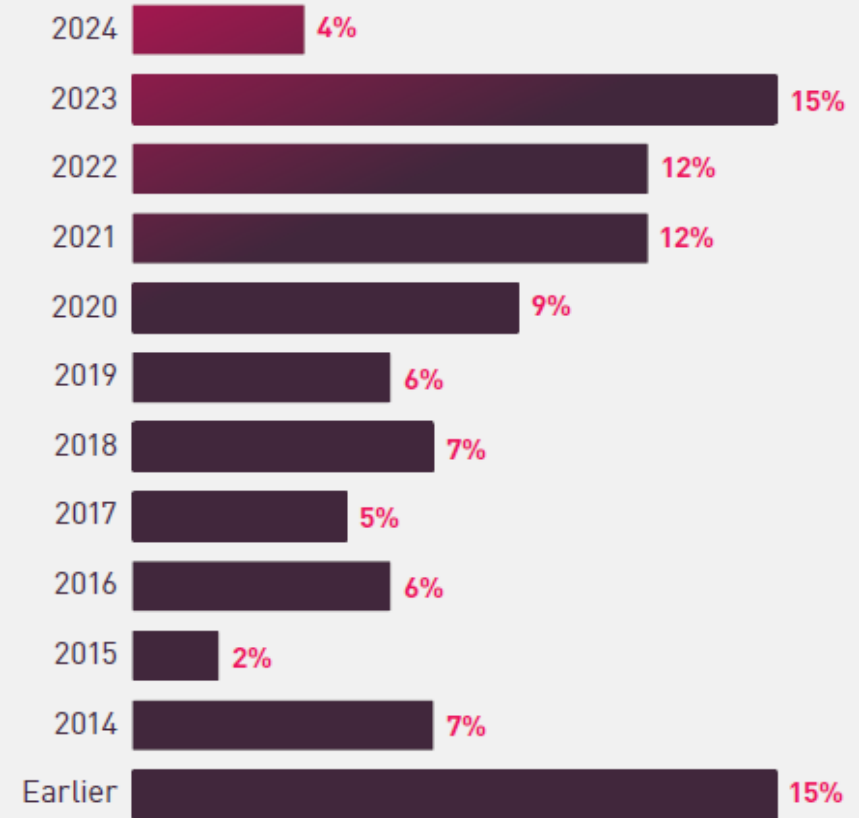
- Utdanning er den mest utsatte sektoren i 5 år på rad
 - Ofte et enkelt mål pga mindre sikkerhet
 - **75% årlig økning i angrep**
- Teknologi sektoren har hatt størst økning av angrep
 - **Maskinvare & Halvledere** + **179%**
 - **Programvare** + **109%**



% av Angrep som utnytter sårbarheter oppdaget pr. år

- Utstrakt bruk av både nye og svært gamle sårbarheter
- Rask utnyttelse av nye sårbarheter (HUSK Å PATCHE!)

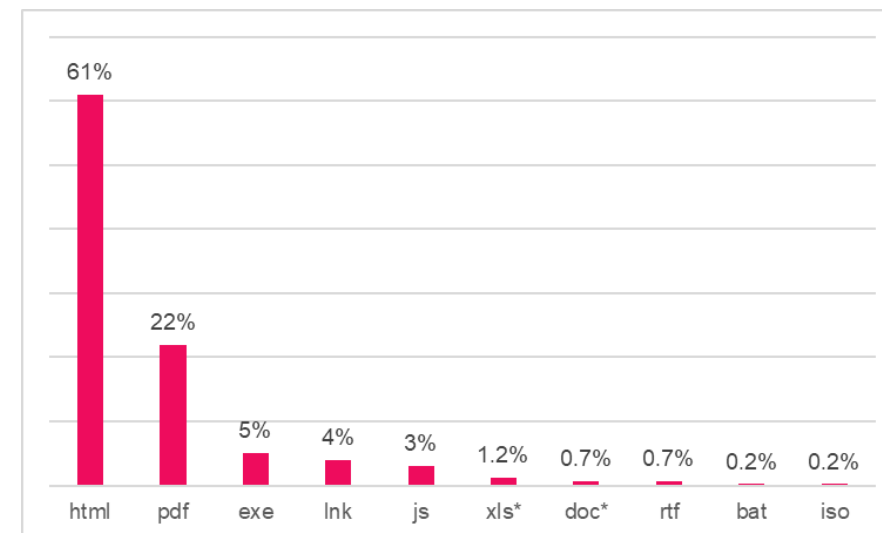
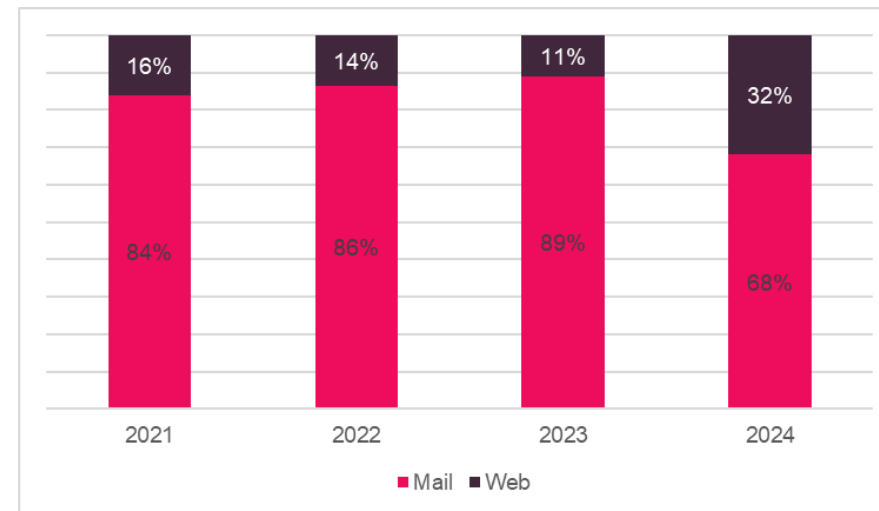
IPS Beskyttelse



1 av 25 angrep i 2024 brukte en sårbarhet som ble offentliggjort i 2024.

Trender for nett- og e-postangrep samt vanlige filtyper

- **Epost** er den vanligste form for angrep med en **vektor på 68%**
- Det er en **økning** i angrep på **web**
- Vanligste ondsinnede filer gjennom epost er **html og pdf**
- **Skadelige** arkiver med **Ink/js** filer øker



E-post sikkerhet

I tillegg til standard

Sandkasse

03

Litt mer om 2025 og fremover

2025 og inn i fremtiden...

Cloud Platforms Become the Backbone of Cyber Security

Cloud-based platforms are increasingly serving as the foundation for cyber security, with AI-driven integration proving more effective than standalone tools. By bringing together various security operations, these platforms reduce complexity, allowing organizations to tackle threats and vulnerabilities in the cloud with greater efficiency and effectiveness. Solutions like CNAPP, ASPM, and DSPM merge to create all-encompassing security posture management (SPM) suites.

As new tools such as Application and Data SPM emerge, they will likely be integrated into a broader Cloud Native Application Protection Platform (CNAPP), potentially leading to the development of what could be called Extended Security Posture Management (XSPM). Integrating Attack Surface Management within this new category illustrates how these platforms can offer more value than a simple collection of point solutions, fundamentally changing how organizations address vulnerabilities.

Rising Risks of AI Misuse and Data Breaches

As AI technologies integrate into personal and workplace environments, concerns about their misuse are growing. This year, the potential for data breaches caused by employees inadvertently sharing sensitive information with AI platforms like ChatGPT or Google's Gemini is a significant risk. Employees might input confidential information, such as financials, to generate reports or analyses, often without realizing that unauthorized individuals could store and access this data. Establishing stricter controls on AI tools within an organization's systems will be crucial for striking a balance between enhancing productivity while ensuring data privacy protections.

AI Powered Financial Crime

2024 began with headlines reporting on sporadic but successful instances of Generative AI powered financial crime. Cyber criminals recognized the potential of GenAI and started investing in its integration into various technological tools, particularly for Business Email Compromise (BEC) and Know Your Customer (KYC) bypass methods. These threats will become more prevalent this year, as cyber criminals are actively working to implement GenAI in these malicious services.

Rising Supply-Chain Attacks on Open-Source Projects

As open-source projects gain popularity, they increasingly become attractive targets for malicious actors aiming to covertly exploit vulnerabilities in widely used software. Following the sophisticated multi-year operation that insert a backdoor into Linux XZ Utils, we can expect new similar attack attempts and the discovery of previously implanted backdoors. This escalating threat highlights the urgent need for enhanced security measures and increased vigilance within the open-source community.

Decentralization of Cyber Crime Ecosystems

Recent successes by law enforcement in combating major ransomware operations and botnets have prompted malicious actors to transition towards smaller, more decentralized networks, methodologies, and operations. Large ransomware projects have restructured into smaller groups, while infostealer-driven ecosystems have emerged as the primary means of facilitating initial access. This decentralization necessitates that defenders adapt their strategies, highlighting the importance of enhanced collaboration and intelligence sharing.

Increased Regulatory Demands and Stricter Cyber Insurance Standards

Organizations will face increasing pressure due to new cyber security regulations, including the EU IoT Regulations, SEC Cyber security Disclosure Rules, the Digital Operational Resilience Act (DORA), and the NIS2 Directive. Compliance with these frameworks will demand a significant investment of time and resources for initiatives such as policy development and new security technologies.

While these regulations aim to improve security measures, they also create additional operational complexities. This requires businesses to devote more attention and effort to meet these standards. Moreover, cyber insurance policies are anticipated to become more stringent, with insurers enforcing stricter controls and compliance requirements as prerequisites for coverage. This will further intensify the regulatory challenges organizations must navigate.

The Growing Cyber Security Talent Gap

The global shortage of cyber security professionals poses a significant challenge for organizations trying to defend against the rising complexity and volume of cyber threats. While organizations invest in versatile security products, the need for more skilled experts to effectively manage and integrate these tools results in a fragmented and inefficient security approach. Dependence on numerous vendors and insufficient in-house knowledge expose organizations to attacks as their security measures become increasingly difficult to manage and less effective. Companies will have to streamline security operations and prioritize the upskilling of staff to maintain resilience.



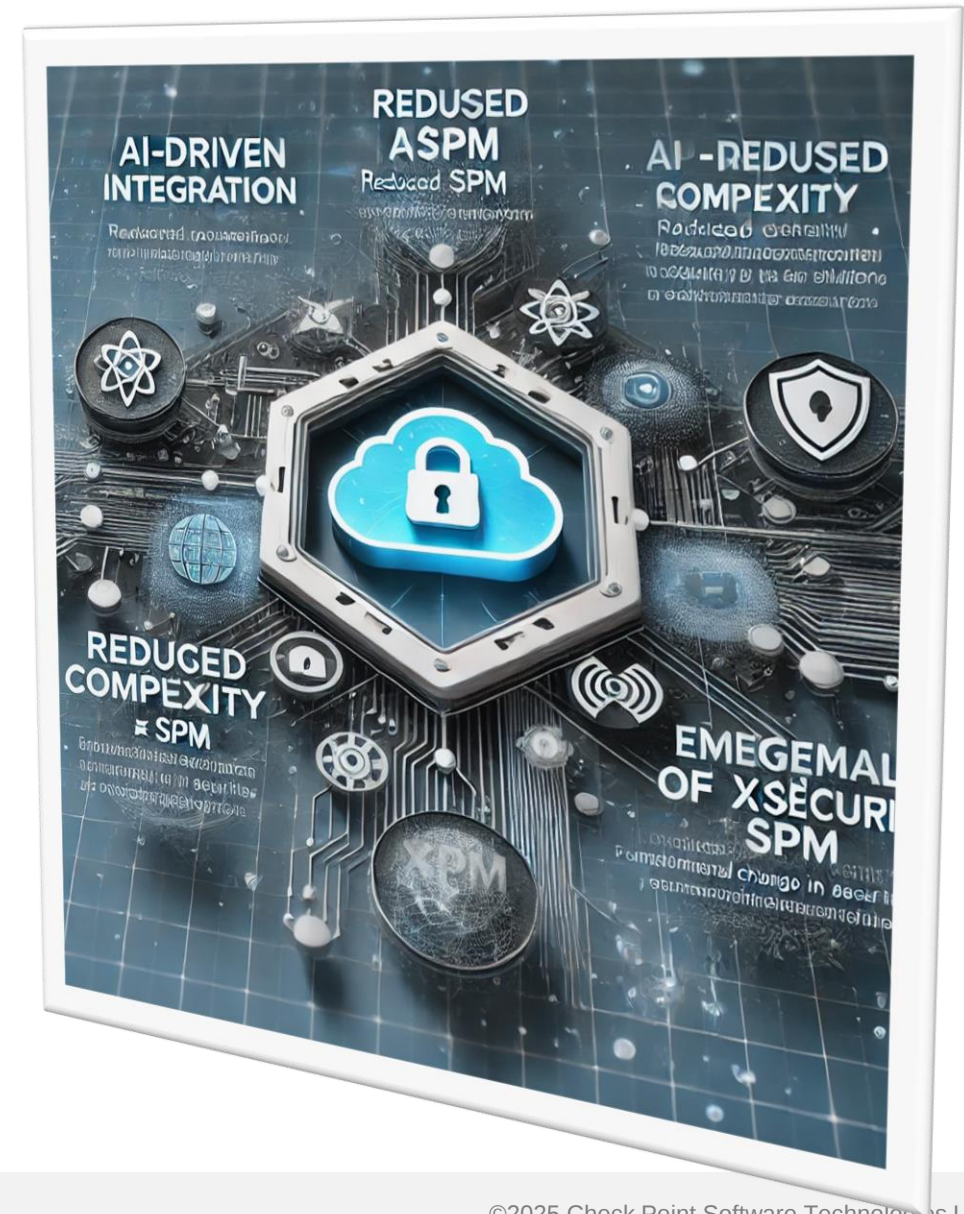
THE STATE OF CYBER SECURITY 2025



Last ned rapport
for detaljer

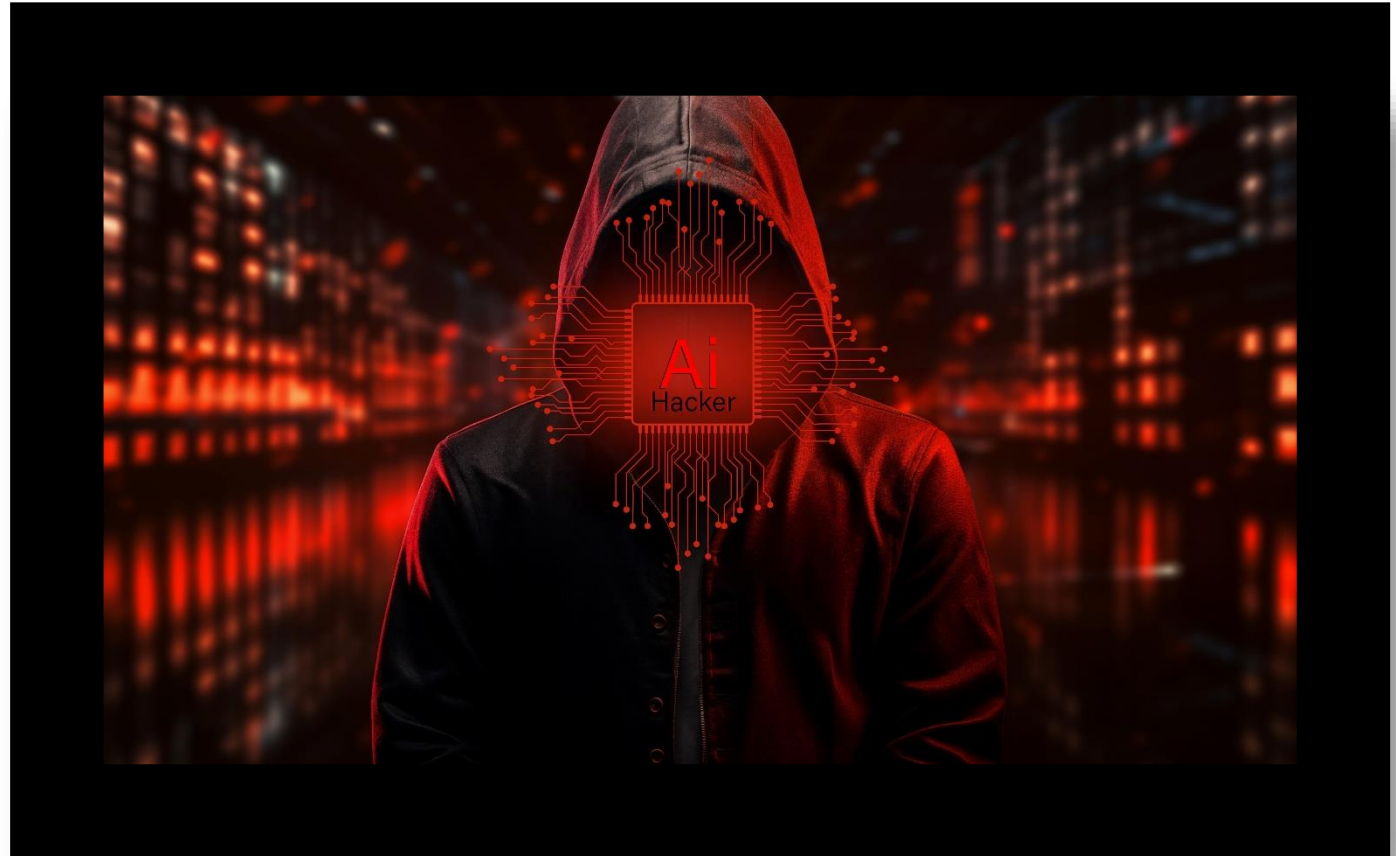
Skyen blir ryggraden innen Cybersikkerhet

- **AI-drevet integrasjon**
 - Mer effektiv enn enkeltstående verktøy
- **Redusert kompleksitet**
 - Samler ulike sikkerhetsoperasjoner
- **CNAPP, ASPM, DSPM → SPM**
 - Helhetlig sikkerhetsstyring
- **Fremvekst av XSPM**
 - Utvidet sikkerhetsstyring med Attack Surface Management
- **Fundamental endring**
 - Mer enn en samling av punktløsninger



Økt risiko for AI misbruk

- **Større AI-integrasjon**
 - AI brukes mer i arbeid og privatliv
- **Høy risiko for datalekkasje**
 - Ansatte deler ubevisst sensitiv informasjon
- **Typisk AI bruk**
 - Phishing, Desinformasjon, Økonomisk kriminalitet, Avansert skadevare, LLM Hijacking
- **Løsning**
 - Strengere kontroller for AI-verktøy
- **Balansen**
 - Produktivitet vs. personvern



Generativ AI og Økonomisk kriminalitet



2024 startet med økt rapportering om AI-drevet, økonomisk kriminalitet

- **Trusselens utvikling**

- Generativ AI brukes til Business Email Compromise (BEC)
- Bruk av AI for å omgå Know Your Customer (KYC) metoder

- **Forventet utvikling**

- Økende trussel gjennom året (2025)
- Cyberkriminelle investerer i AI-teknologi for ondsinnede tjenester

Åpen Kildekode

Økt Risiko for Bakdører

- **Trusselens Utvikling**

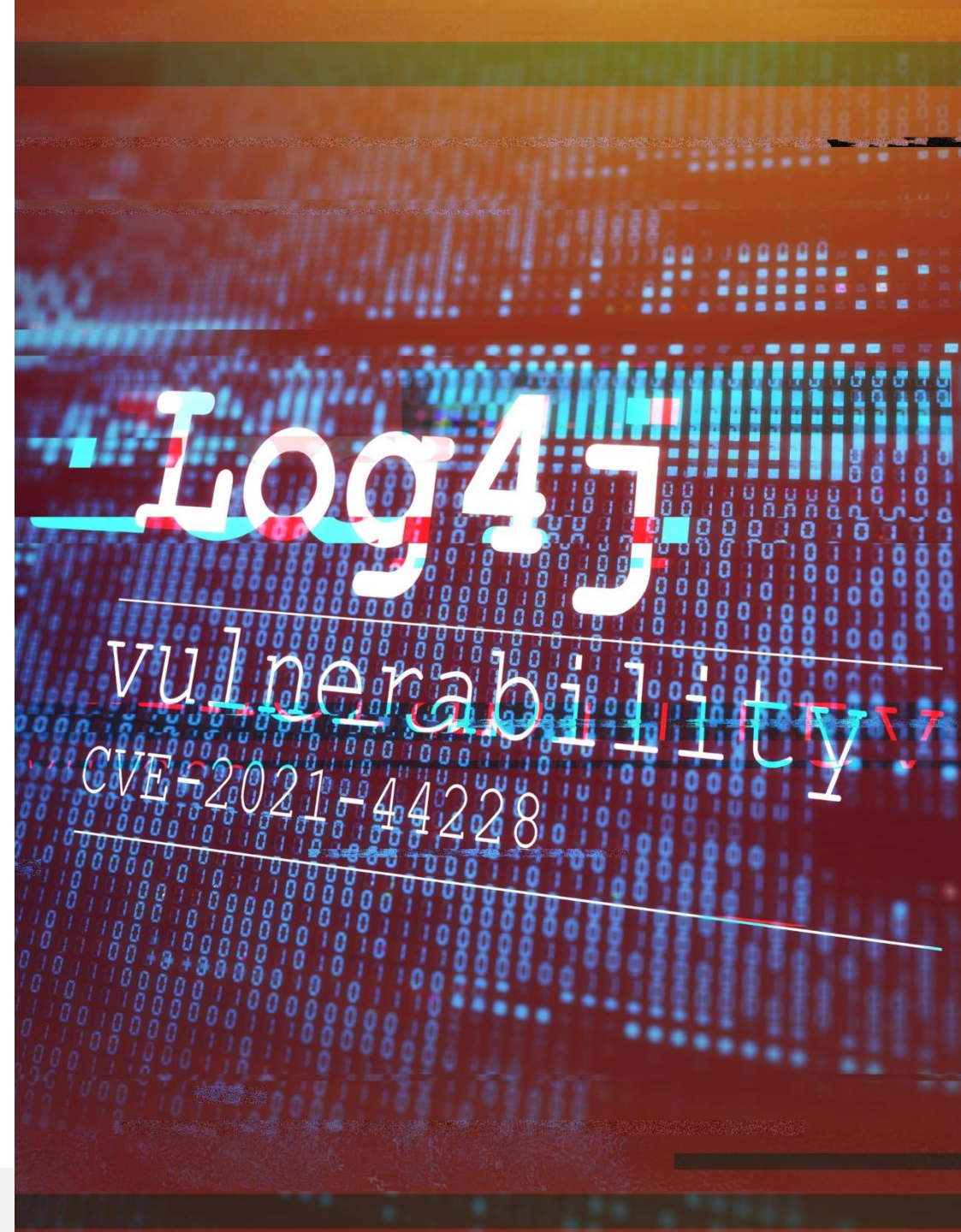
- Åpen kildekode-prosjekter blir attraktive mål for ondsinnede aktører.
- Eksponert for sårbarheter i programvare.

- **Eksempel**

- Sofistikert flerårig operasjon som satte inn bakdør i Linux XZ Utils.
- Forvent nye angrepsforsøk og bakdører.

- **Hva dette betyr**

- Eskalerende trussel mot åpen kildekode.
- Økt behov for styrkede sikkerhetstiltak og årvåkenhet i fellesskapet.



Desentralisering av økosystemer



- **Endringer i Trusselbildet**

- Ransomware og botnett har blitt desentraliserte
- Større grupper er delt opp i mindre grupper
- Infostjelere er hovedmetoden for å skaffe tilgang

- **Betydning for Forsvarere**

- Desentralisering krever tilpasning av strategier
- Økt behov for samarbeid og informasjonsdeling

Flere regulatoriske krav

- **Nye Reguleringer**

- EU IoT-reguleringene
- SEC Cyber Security Closure
- Digital Operational Resilience Act (DORA)
- NIS2-direktiv

- **Krav og Investeringer**

- Økt tid og ressursbehov for policyutvikling
- Behov for investering i nye sikkerhetsteknologier

- **Utfordringer**

- Organisasjoner må tilpasse seg for å sikre overholdelse
- Økt administrativ og teknologisk belastning



Strengere krav til Cyberforsikring



- **Strengere Forsikringskrav**

- Strengere kontroller og krav til overholdelse fra forsikringsselskapene som forutsetninger for dekning

- **Samlet Utfordring**

- Økt regulatorisk press på organisasjoner
- Nødvendigheten av å navigere både nye reguleringer og strengere forsikringskrav

Økende utfordring: Mangelen på kompetanse

- **Effektivitet og Fragmentering**

- Organisasjoner investerer i sikkerhetsprodukter, men ekspertmangel fører til ineffektiv drift.

- **Konsekvenser**

- Avhengighet av mange leverandører og mangel på intern kompetanse
- Økt eksponering for angrep og redusert effektivitet i sikkerhetstiltakene

- **Tiltak**

- Strømlinjeforme/Outsource SOC
- Prioritere kompetanseheving og automatisere for å opprettholde motstandskraft
- Benytte AI for effektivisering



04

CISO anbefalinger

Noen råd på veien fra CISO til CISO

Anbefalinger til og fra CISO

- Bygg sikkerhet i lag-på-lag
- Prioriter sikkerhet i sky
- Bruk AI for å stoppe trusler
- Få full oversikt over angrepsflate
- Etabler digital tillit

Implementer sikkerhet i flere lag bestående av redundans, katastrofesikring, sikkerhetskopiering av data, endepunkter, nettverk, sky, e-post og opplæring av ansatte.

Bruk av EDR/MDR/XDR-verktøy kan hjelpe med å identifisere og isolere trusler tidlig.

Oppretthold streng tilgangskontroll og bruk av minst privilegerte prinsipper for å begrense potensialet for angrep.

Sørg for oppdatering av programvare og systemer, men ikke glem å teste oppdateringer før det rulles ut i stor skala.

Gjennomfør regelmessig sikkerhetsvurderinger og beredskapsøvelser.



Anbefalinger til og fra CISO

- Bygg sikkerhet i lag-på-lag
- **Prioriter sikkerhet i sky**
- Bruk AI for å stoppe trusler
- Få full oversikt over angrepsflate
- Etabler digital tillit

Prioriter API-sikkerhet, identitet og en Zero Trust arkitektur for å adressere sårbarheter i skyen.

Bruk en kraftig API-gateway (WAF/WAP) og gjennomfør regelmessig revisjoner for å redusere risikoen for data-lekkasje.

Implementering av minst privilegert tilgang og multi-faktor autentisering er avgjørende for å sikre ressursene.

En Zero Trust modell forbedrer sikkerhet ved å verifisere brukere og enheter før tilgang.

Hindre feilkonfigurasjoner, rettigheter og tilgangsnivåer med Posture Management verktøy (CSPM/CWPP).



Anbefalinger til og fra CISO

- Bygg sikkerhet i lag-på-lag
- Prioriter sikkerhet i sky
- **Bruk AI for å stoppe trusler**
- Få full oversikt over angrepsflate
- Etabler digital tillit

Bruk avansert kunstig intelligens for å oppdage og stoppe angrep.

Med robuste, AI-drevne systemer kan man effektivt identifisere og redusere potensielle trusler før de eskalerer.

Denne proaktive tilnærmingen innebærer implementering av automatiserte løsninger som utnytter AI i sanntid for å hindre trusler.

Slike systemer forbedrer den generelle sikkerheten og effektiviserer responsen, som igjen gjør det mulig å handle raskt og effektivt mot nye utfordringer.



Anbefalinger til og fra CISO

- Bygg sikkerhet i lag-på-lag
- Prioriter sikkerhet i sky
- Bruk AI for å stoppe trusler
- Få full oversikt over angrepsflate
- Etabler digital tillit

Kriminelle utnytter sårbarheter ifm BYOD praksis og skybaserte applikasjoner, noe som øker risikoen for å bli kompromittert pga problemer som hardkodete passord og generelt svak autentisering.

De bruker ofte en legitim identitet og kjente verktøy, som visker ut grensen mellom vanlig brukeraktivitet og ondsinnede handlinger.

Man må forstå kobling mellom identitet, sky, endepunkt og databeskyttelse og identifisere truslene på tvers av flere systemer.

En enhetlig og AI drevet plattform for sikkerhet, forbedrer synlighet og kontroll, samt sørger for økt beskyttelse.



Anbefalinger til og fra CISO

- Bygg sikkerhet i lag-på-lag
- Prioriter sikkerhet i sky
- Bruk AI for å stoppe trusler
- Få full oversikt over angrepsflate
- Etabler digital tillit

Man bør etablere et tillitsprogram for å dekke de krav dagens raskt skiftende regelverk påfører bedriften.

Å implementere automatisering for regulatoriske krav kan effektivisere overholdelse av strenge regler og redusere menneskelige feil under revisjoner og rapportering.

Klassifisering av data tillater virksomheter å opprettholde kontroll over sensitiv informasjon.

Ved å inkludere personvern «by design» kan man proaktivt beskytte kundedata, forbedre sikkerhet, og ligge i forkant av digitale trusler.

Denne tilnærmingen fremmer et sterkt rammeverk som til slutt bygger kundens tillit.



Anbefalinger til og fra CISO

- Etabler et system for sårbarhet og risikostyring
- Velg en leverandør du stoler på
- Effektiviser sikkerheten
- Fokuser på motstandskraft og hendelseshåndtering

Den raske fremveksten av nye sårbarheter, spesielt zeroday-angrep, utgjør en betydelig utfordring for håndtering av sårbarheter.

Systemer, tjenester og kritiske løsninger, som eventuelt er eksponert ut mot Internett bør være hovedfokus.

For å effektivt håndtere disse risikoene er det viktig å vurdere trusselnivåene og prioritere dem deretter, f.eks i forhold til patching.

Bruk av trusselintelligens sammen med overvåking av ekstern angrepsflate gir verdifull innsikt i hvordan motstandere oppfatter sikkerhetstiltakene dine.

Med denne innsikten kan du implementere forebyggende strategier.



Anbefalinger til og fra CISO

- Etabler et system for sårbarhet og risikostyring
- **Velg en leverandør du stoler på**
- Effektiviser sikkerheten
- Fokuser på motstandskraft og hendelseshåndtering

Velg en sikkerhetsprodusent som formidler digital trygghet.

Se etter et selskap med dokumentert merittliste av effektiv sikkerhetspraksis og lave sårbarhetsrater.

Prioriter leverandører som sørger for raske patchutgivelser, slik at man kan håndtere potensielle trusler raskt.

I tillegg vurder selskapets strategi for hendelseshåndtering, respons og historikk ifm med eventuelle sikkerhetsbrudd.



YOU DESERVE THE BEST SECURITY



Anbefalinger til og fra CISO

- Etabler et system for sårbarhet og risikostyring
- Velg en leverandør du stoler på
- **Effektiviser sikkerheten**
- Fokuser på motstandskraft og hendelseshåndtering

Gitt mangelen på personell og kompetanse innen cybersikkerhet, er AI avgjørende for effektiviteten, slik at teamene bedre kan administrere og prioritere trusselhåndtering.

AI-verktøy kan automatisere repeterende oppgaver og minimere tid brukt på oppgaver som f.eks hendelseanalyse og feilsøking.

Fagfolk kan fokusere på strategisk innovasjon og proaktive tiltak med strømlinjeformede prosesser.



Anbefalinger til og fra CISO

- Etabler et system for sårbarhet og risikostyring
- Velg en leverandør du stoler på
- Effektiviser sikkerheten
- Fokuser på motstandskraft og hendelseshåndtering

Sørg for at ulike deler av bedriften er effektivt adskilt.

Denne tilnærmingen vil forbedre din hendelsesrespons i tilfelle et angrep.

Regelmessig vurdere og oppdatere katastrofeplaner for å minimere forstyrrelser forårsaket av nettangrep eller annen nedetid.

Brukerutdanning er avgjørende for å forhindre skadelig programvare. Ansatte bør være klar over kildene til filer og e-poster og om de kan stole på avsendere.

Den vanligste angrepsvektoren for løsepengevirus er fortsatt phishing-e-poster og ondsinnede websider.

Økt brukerbevissthet forhindrer ofte angrep. Lær opp brukerne dine og oppmuntre dem til å rapportere noe uvanlig eller mistenkelig øyeblikkelig.





- Digitale og Hybride trusler øker
- AI er over alt !!
- Utekontor og endepunkter angripes
- Hybrid infrastruktur er sårbar



- Digitale og Hybrid trusler øker

Få kontroll på IDENTITET

og egentlig alt annet også 😊

- Hybrid infrastruktur er sårbar

Last ned hele rapporten her



THE STATE OF CYBER
SECURITY 2025



Spørsmål?

Pål H. Aaserudseter | paala@checkpoint.com

YOU DESERVE THE BEST SECURITY