bravo

VI KOMBINERER IT OG AV PÅ MÅTER INGEN ANDRE GJØR. VI KALLER DET IT-MAGI.

Alt for din digitale hverdag, samlet på et sted.

IT-sikkerhetsguide.

1.0 Introduksjon.
- 1.1 Hva er IT-sikkerhet?
- 1.2 Hvorfor er IT-sikkerhet viktig?

2.0 Digitale trusler.
- 2.1 Skadelig programvare (malware)
  - 2.1.1 Ransomware
- 2.2 Phising
- 2.3 DDoS-angrep (distributed denial of service)
- 2.4 Zero-day sårbarheter
- 2.5 Insider-trusler
- 2.6 Nettverkstrusler

3.0 Fysiske trusler mot digital infrastruktur.
- 3.1 Social engineering
- 3.2 Fysisk tilgang til data og maskinvare
- 3.3 Mobile enheter
- 3.4 Sikkerhetskopiering og gjenoppretting av data
- 3.5 SIkring av fysiske lokasjoner

4.0 Beste praksis for IT-sikkerhet.
- 4.1 Passord
- 4.2 Oppdatering og patching av programvare
- 4.3 Sikkerhetsopplæring for ansatte
- 4.4 Kryptering av data
- 4.5 Nettverkssegmentering og brannmurer

bravo

VI KOMBINERER IT OG AV PÅ MÅTER INGEN ANDRE GJØR. VI KALLER DET IT-MAGI.

Alt for din digitale hverdag, samlet på et sted.

5.0 Sikkerhetsverktøy og teknologier.

- 5.1 Antivirus og antimalware-programvare
- 5.2 Intrusion detection systems (IDS) og intrusion prevention systems (IPS)
- 5.3 Sikkerhetsinformasjon og hendelseshåndtering (SIEM)
- 5.4 Virtuelle private nettverk (VPN)
- 5.5 Multifaktorautentisiering (MFA)
- 5.6 Sikerhetskopieringsløsninger

6.0 Regelverk og standarder.

- 6.1 General data protection regulation (GDPR)
- 6.2 ISO/IEC 27001
- 6.3 NIST cybersecurity framework
- 6.4 Payment card industry data security standard (PCI DSS)

7.0 Håndtering av sikkerhetshendelser.

- 7.1 Incident reponse plan (IRP)
- 7.2 Oppdagelse og varsling
- 7.3 Analyse og containment
- 7.4 Gjenoppretting og rapportering
- 7.5 Læring og forbedring

8.0 Fremtidige trender innen IT-sikkerhet.

- 8.1 Kunstig intelligens og maskinlæring
- 8.2 Skybasert sikkerhet (cloud security)
- 8.3 IoT-sikkerhet
- 8.4 Kvantedatamaskiner og kryptering
- 8.5 Personvern som integrert del av IT-sikkerhet (privacy by design)

1.0 Introduksjon.

1.1 Hva er IT-sikkerhet?

IT-sikkerhet handler om å beskytte dine digitale ressurser – som data, programvare, nettverk og maskinvare – mot uautoriserte tilgang, modifikasjon, tyveri eller skade. Dette inkluderer en rekke teknikker og teknologier, fra kryptering og brannmurer til fysisk sikring av serverrom. Målet er å sikre konfidensialitet, integritet og tilgjengelighet av dataene dine, slik at bare autoriserte brukere har tilgang, og at informasjonen forblir uendret og tilgjengelig når den trengs.

1.1 Hvorfor er IT-sikkerhet viktig?

I en tid hvor data er blitt en av de mest verdifulle ressursene vi har, er IT-sikkerhet avgjørende. Et sikkerhetsbrudd kan føre til tap av sensitiv informasjon, økonomiske tap, skade på omdømmet og i verste fall juridiske konsekvenser. Dette gjelder ikke bare for store selskaper, men også for små bedrifter og enkeltpersoner. Uten adekvate sikkerhetstiltak kan du risikere at uvedkommende får tilgang til systemene dine, noe som kan få alvorlige konsekvenser.

2.0 Digitale trusler.

2.1 Skadelig programvare (malware)

Skadelig programvare er en bred kategori som inkluderer virus, trojanere, spyware og ransomware, blant annet. Disse programmene kan utføre en rekke ondsinnede handlinger, som å stjele data, spionere på deg, ta kontroll over systemet ditt eller kryptere filene dine for løsepenger. Malware kan infisere systemet ditt gjennom vedlegg i e-poster, nedlastede filer eller til og med besøkte nettsteder. Et sterkt antivirusprogram, kombinert med forsiktighet når du åpner ukjente filer, kan beskytte deg mot mange typer malware.

2.1.1 Ransomware

Ransomware er en type malware som krypterer filene dine og krever løsepenger for å låse dem opp. Dette kan lamme en virksomhet fullstendig hvis de ikke har tilgang til sikre sikkerhetskopier. Ransomware spres ofte via e-poster med ondsinnede vedlegg eller lenker til infiserte nettsteder. Regelmessig sikkerhetskopiering av data og opplæring i å gjenkjenne mistenkelige e-poster er essensielt for å beskytte seg mot denne typen angrep.

2.2 Phising

Phishing-angrep er forsøk på å lure deg til å avsløre sensitiv informasjon, som passord eller kredittkortnummer, ved å utgi seg for å være en pålitelig kilde. Dette skjer ofte gjennom falske e-poster eller nettsider som ser ut som legitime. Phishing kan være svært overbevisende, men det er ofte små tegn som kan avsløre dem, som dårlig grammatikk, merkelige avsenderadresser eller uvanlige forespørsler. Å være skeptisk til uoppfordrede meldinger og å dobbeltsjekke avsenders legitimitet er viktige beskyttelsestiltak.

2.3 DDoS-angrep (distributed denial of service)

Et DDoS-angrep fungerer ved å overvelde et nettsted eller en tjeneste med så mye trafikk at det blir utilgjengelig for legitime brukere. Dette kan føre til tap av inntekter og skade på omdømmet, spesielt hvis tjenesten din er avhengig av konstant oppetid. DDoS-angrep er vanskelige å stoppe, men beskyttelsestiltak som trafikkfiltrering, bruk av DDoS-beskyttelsestjenester, og å ha en beredskapsplan kan hjelpe med å minimere effektene.

2.4 Zero-day sårbarheter

Zero-day sårbarheter er sikkerhetshull i programvare som ennå ikke er oppdaget av utviklerne, men som angripere allerede har begynt å utnytte. Disse sårbarhetene er spesielt farlige fordi de kan bli brukt til å lansere angrep før noen har en sjanse til å lage en patch. For å beskytte seg mot zero-day angrep er det viktig å holde programvaren oppdatert og bruke sikkerhetsløsninger som kan oppdage uvanlig oppførsel i systemet.

2.3 Insider-trusler

Insider-trusler kommer fra personer innenfor organisasjonen som misbruker sin tilgang til systemer og data. Dette kan være nåværende eller tidligere ansatte, samarbeidspartnere eller entreprenører som har tilgang til sensitiv informasjon. Insidere kan lekke informasjon, sabotere systemer, eller stjele data for egen vinning eller skade på organisasjonen. Strenge tilgangskontroller, overvåkning og regelmessig revisjon av brukerrettigheter kan bidra til å redusere risikoen for slike trusler.

2.3 Nettverkssikkerhet

Nettverkssikkerhet handler om å beskytte data som flyter gjennom nettverket ditt mot uautoriserte tilgang eller modifikasjoner. Dette inkluderer bruk av brannmurer, VPN-er, Intrusion Detection Systems (IDS) og andre verktøy for å overvåke og sikre nettverket ditt. En godt sikret nettverksinfrastruktur beskytter deg mot mange typer angrep, inkludert datatyveri, malware-distribusjon og DDoS-angrep.

3.0 Fysiske trusler.

3.1 Social engineering

Social Engineering er kunsten å manipulere mennesker til å gi opp informasjon eller utføre handlinger som de ellers ikke ville gjort. Dette kan inkludere phishing-angrep, men også fysiske forsøk som tailgating, hvor en angriper følger en autorisert person inn i en sikret bygning uten å bli oppdaget. For å beskytte seg mot social engineering er det viktig med regelmessig opplæring av ansatte, slik at de blir bevisste på disse truslene og vet hvordan de skal håndtere dem.

3.2 Fysisk tilgang til data og maskinvare

Fysisk tilgang til maskinvare kan være like farlig som digital tilgang. En angriper som får fysisk tilgang til servere, datamaskiner eller andre enheter, kan stjele data, installere skadelig programvare, eller ødelegge utstyr. Beskyttelse mot slike trusler inkluderer sikring av kontorer og serverrom med låser, adgangskontrollsystemer, og overvåkningskameraer. Å begrense hvem som har fysisk tilgang til sensitivt utstyr, er en grunnleggende sikkerhetspraksis.

3.3 Sikkerhet for mobile enheter

Mobiltelefoner og nettbrett er sårbare mål for tyveri og hacking, spesielt fordi de ofte inneholder mye sensitiv informasjon og er utsatt for tap eller tyveri. Sikring av mobile enheter inkluderer bruk av passord eller biometrisk lås, kryptering av data, og fjernsletting i tilfelle enheten blir stjålet. Dette bidrar til å beskytte informasjonen selv om enheten havner i feil hender.

3.4 Sikring av fysiske lokasjoner

Fysiske lokasjoner, som kontorer og datasentre, må sikres for å forhindre uautorisert tilgang til sensitiv informasjon og utstyr. Dette kan innebære alt fra låsing av dører og installering av adgangskontrollsystemer til bruk av sikker lagring for sensitive dokumenter og medier. Fysisk sikkerhet er en viktig del av en helhetlig IT-sikkerhetsstrategi og bør ikke overses.

3.5 Sikkerhetskopiering og gjenoppretting av data

Å ha regelmessige sikkerhetskopier av dataene dine er en av de beste forsvarene mot tap av data, enten det skyldes ransomware, fysisk skade på maskinvare, eller andre problemer. Sikkerhetskopier bør lagres på et sikkert sted, adskilt fra hovedsystemene, slik at de ikke blir påvirket av samme katastrofe som hoveddataene. En godt planlagt gjenopprettingsprosess sørger for at du raskt kan komme tilbake til normal drift etter et brudd eller tap av data.

4.0 Beste praksis for IT-sikkerhet.

4.1 Bruk av sterke passord og tofaktorautentisering

Sterke passord er første forsvarslinje mot uautorisert tilgang. Et sterkt passord bør være langt, komplekst og unikt for hver konto. Men selv sterke passord kan bli kompromittert, derfor er tofaktorautentisering (2FA) et viktig tillegg. 2FA krever at brukeren oppgir to typer informasjon før tilgang gis, for eksempel et passord og en kode sendt til mobiltelefonen. Dette gir et ekstra sikkerhetslag, selv om passordet blir stjålet.

4.2 Oppdatering og patching av programvare

Programvareoppdateringer og sikkerhetspatcher er avgjørende for å beskytte systemene dine mot kjente sårbarheter. Når en ny sårbarhet oppdages, jobber utviklere raskt for å lage en patch som tetter hullet. Hvis du ikke installerer disse oppdateringene, forblir systemet ditt sårbart for angrep. En automatisert oppdateringsprosess kan bidra til å sikre at alle systemer alltid er oppdatert.

4.3 Fortløpende sikkerhetsopplæring for ansatte

Ansatte er ofte den svakeste lenken i sikkerhetskjeden, men med riktig opplæring kan de bli en av de sterkeste. Regelmessig sikkerhetsopplæring hjelper ansatte med å gjenkjenne trusler som phishing-e-poster, skadelige vedlegg og social engineering-angrep. Ved å oppdatere opplæringen regelmessig og inkludere praktiske øvelser, kan du sikre at teamet ditt er forberedt på de siste truslene.

4.4 Kryptering av data

Kryptering er prosessen med å konvertere data til en uleselig form som kun kan dekrypteres av autoriserte parter med riktig nøkkel. Dette beskytter dataene dine både i transit (når de sendes over nettverket) og i hvile (når de lagres). Kryptering bør være en standardpraksis for all sensitiv informasjon for å forhindre at dataene blir lest av uvedkommende, selv om de skulle få tak i dem.

4.5 Nettverkssegmentering og brannmurer

Nettverkssegmentering innebærer å dele opp nettverket ditt i mindre deler, hver med sine egne sikkerhetsregler. Dette begrenser hvor langt en angriper kan komme hvis de klarer å få tilgang til en del av nettverket. Brannmurer fungerer som en barriere mellom nettverket ditt og eksterne trusler, og kontrollerer hvilken trafikk som får lov til å komme inn og ut. Sammen gir disse tiltakene et robust forsvar mot nettverksbaserte angrep.

5.0 Sikkerhetsverktøy & teknologier.

5.1 Antivirus og antimalware-programvare

Antivirus- og antimalware-programvare er essensielle verktøy for å beskytte datamaskiner og nettverk mot skadelig programvare. Disse programmene skanner systemene dine for kjente trusler og fjerner dem før de kan forårsake skade. Det er viktig å holde denne programvaren oppdatert, slik at den kan beskytte mot de nyeste truslene. Selv om de ikke er en perfekt løsning, gir de en viktig beskyttelse mot mange vanlige typer malware.

5.2 Intrusion detection systems (IDS) og intrusion prevention systems (IPS)

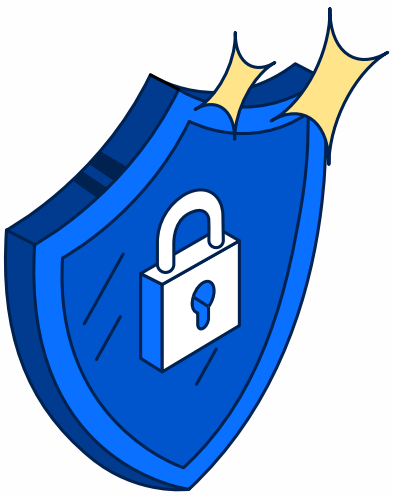
IDS og IPS er sikkerhetsverktøy som overvåker nettverkstrafikk for mistenkelig aktivitet. IDS varsler deg hvis det oppdages noe mistenkelig, mens IPS kan gå et skritt videre og automatisk blokkere trusler før de får gjort skade. Disse systemene er viktige for å oppdage og reagere på angrep som har klart å komme seg forbi andre sikkerhetslag.

5.3 Sikkerhetsinformasjon og hendelseshåndtering (SIEM)

SIEM-systemer samler inn og analyserer sikkerhetsdata fra hele nettverket ditt i sanntid, og gir deg innsikt i hva som skjer i systemene dine. SIEM-verktøy kan oppdage trusler som andre sikkerhetssystemer kan gå glipp av, og de gir deg også de verktøyene du trenger for å respondere raskt og effektivt på sikkerhetshendelser. SIEM er et kraftig verktøy for å holde oversikt over sikkerhetsstatusen til et komplekst nettverk.

5.4 Virtuelle private nettverk (VPN)

Et VPN skaper en sikker, kryptert forbindelse over et mindre sikkert nettverk, som internett. Dette beskytter dataene dine mot avlytting når du jobber eksternt eller kobler deg til offentlige nettverk. VPN-er er spesielt nyttige for å beskytte sensitive informasjon når den sendes over usikre forbindelser, og bør være en standard praksis for alle som jobber utenfor kontoret. Microsoft 365-brukere har 5GB VPN inkludert i lisensen sin via Edge Secure Network VPN. Edge Secure Network bruker VPN-teknologi for å kryptere internettforbindelsen din, skjule posisjonen din og IP-adressen din, og holde surfeaktiviteten din privat, slik at tredjeparter og hackere ikke kan få tilgang til sensitive data. Dette betyr at du kan foreta kjøp på nettet, fylle ut personlige skjemaer og surfe på nettsider med trygghet om at dårlige skuespillere ikke kan se dataene dine.



5.5 Multifaktorautentisering (MFA)

MFA legger til et ekstra sikkerhetslag ved å kreve to eller flere bekreftelsesfaktorer før en bruker får tilgang til en konto eller et system. Dette kan inkludere noe brukeren vet (som et passord), noe de har (som en SMS-kode eller en autentiseringsapp), eller noe de er (som et fingeravtrykk). MFA gjør det mye vanskeligere for angripere å få tilgang til systemene dine, selv om de har klart å stjele et passord.

5.6 Sikkerhetskopieringsløsninger

Sikkerhetskopieringsløsninger sikrer at du alltid har en kopi av viktige data tilgjengelig, slik at du kan gjenopprette systemene dine raskt etter et brudd eller tap av data. Det er viktig å automatisere sikkerhetskopieringsprosessen og regelmessig teste gjenopprettingsprosedyrene for å sikre at de fungerer som forventet. Ved å lagre sikkerhetskopiene på et sikkert, adskilt sted, kan du beskytte dem mot samme trussel som påvirket hovedsystemene dine.

6.0 Regelverk og standarder.

6.1 General data protection regulation (GDPR)

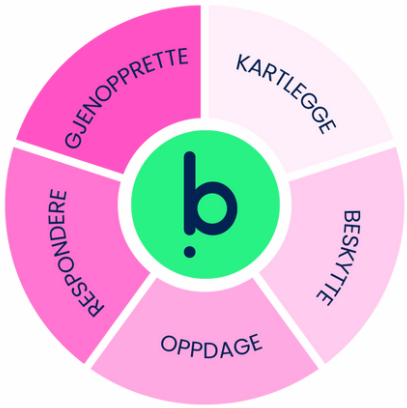
GDPR er en omfattende personvernlovgivning som gjelder for alle selskaper som behandler data om individer i EU. Loven krever at selskaper tar sterke tiltak for å beskytte personopplysninger, inkludert bruk av kryptering, begrensning av datainnsamling og sikring av at data bare brukes til de formålene de ble samlet inn for. Manglende overholdelse av GDPR kan føre til betydelige bøter, så det er viktig å forstå og følge disse reglene hvis du behandler data om EU-borgere.

6.2 ISO/IEC 27001

ISO/IEC 27001 er en internasjonal standard for informasjonssikkerhet som gir retningslinjer for hvordan du skal etablere, implementere, vedlikeholde og kontinuerlig forbedre et informasjonssikkerhetsstyringssystem (ISMS). Å følge denne standarden hjelper organisasjoner med å identifisere risikoer, implementere kontroller for å håndtere disse risikoene, og sikre at informasjonen deres er godt beskyttet. Sertifisering i ISO/IEC 27001 kan også være en måte å vise kunder og partnere at du tar sikkerhet på alvor.

6.3 NIST cybersecurity framework

NIST-rammeverket er en veiledning utviklet av National Institute of Standards and Technology (NIST) i USA, som hjelper organisasjoner med å forstå, administrere og redusere risikoen forbundet med cybersikkerhet. Rammeverket er delt inn i fem kjernefunksjoner: identifisere, beskytte, oppdage, respondere, og gjenopprette. Ved å følge dette rammeverket kan organisasjoner bygge en robust cybersikkerhetsstrategi som er tilpasset deres spesifikke behov og risikoer.



6.4 PCI DSS (payment card industry data security standard)

PCI DSS er en sikkerhetsstandard utviklet for å beskytte betalingskortdata. Den gjelder for alle selskaper som lagrer, behandler eller overfører kredittkortinformasjon. PCI DSS krever at selskaper implementerer en rekke sikkerhetstiltak, inkludert kryptering av data, brannmurer, tilgangskontroll og regelmessig overvåking av nettverk. Overholdelse av PCI DSS er avgjørende for å unngå databrudd og bøter, samt for å opprettholde tilliten til kundene.

7.0 Håndtering av sikkerhetshendelser.

7.1 Incident response plan

GDPR er en omfattende personvernlovgivning som gjelder for alle selskaper som behandler data om individer i EU. Loven krever at selskaper tar sterke tiltak for å beskytte personopplysninger, inkludert bruk av kryptering, begrensning av datainnsamling og sikring av at data bare brukes til de formålene de ble samlet inn for. Manglende overholdelse av GDPR kan føre til betydelige bøter, så det er viktig å forstå og følge disse reglene hvis du behandler data om EU-borgere.

7.2 Oppdagelse og varsling

Tidlig oppdagelse av sikkerhetshendelser er avgjørende for å begrense skader. Dette innebærer bruk av overvåkingsverktøy som kan oppdage mistenkelig aktivitet i sanntid, samt et klart system for varsling som sikrer at de rette personene blir informert så snart et problem oppstår. Jo raskere du oppdager og svarer på en trussel, desto mindre sannsynlig er det at den vil forårsake alvorlig skade.

7.3 Analyse og containment

Når en sikkerhetshendelse er oppdaget, må du raskt analysere situasjonen for å forstå omfanget av angrepet og hvordan det skjedde. Containment handler om å isolere den berørte delen av systemet for å forhindre at trusselen sprer seg. Dette kan innebære å koble fra infiserte maskiner fra nettverket, deaktivere kontoer som er kompromittert, eller stanse spesifikke tjenester. Containment er et kritisk skritt for å sikre at skaden ikke eskalerer.

7.4 Gjenoppretting og rapportering

Etter at trusselen er inneholdt, må du begynne gjenopprettingsprosessen. Dette kan inkludere å gjenopprette data fra sikkerhetskopier, reparere systemer, og sikre at alle sårbarheter som ble utnyttet, er fikset. Det er også viktig å dokumentere hele hendelsesforløpet i en rapport som beskriver hva som skjedde, hvilke tiltak som ble tatt, og hva som kan gjøres for å forhindre lignende hendelser i fremtiden.

7.5 Læring og forbedring

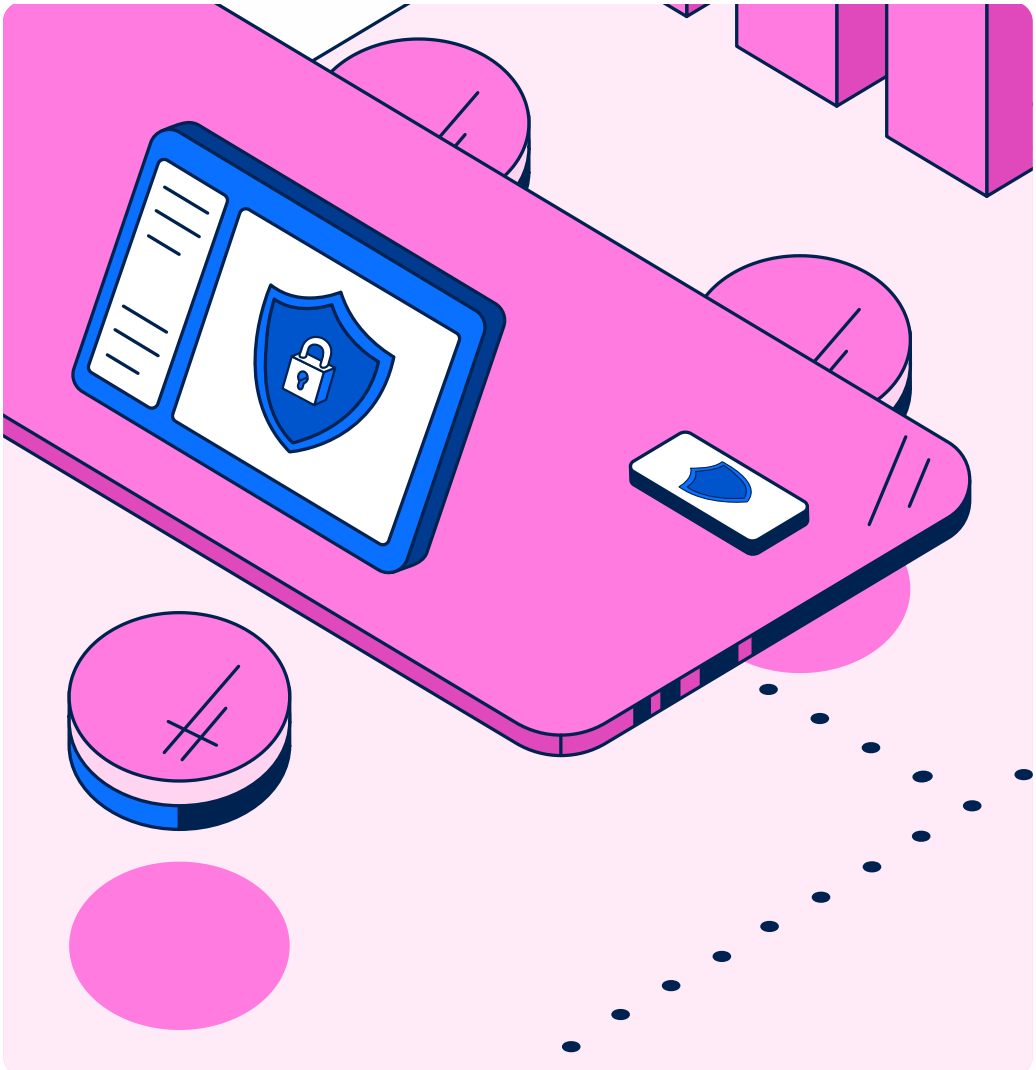
Når en sikkerhetshendelse er håndtert, er det viktig å gjennomføre en grundig gjennomgang for å lære av hendelsen. Dette inkluderer å evaluere hva som fungerte bra, hva som kunne vært gjort bedre, og hvilke nye tiltak som kan implementeres for å forbedre sikkerheten fremover. Læring og kontinuerlig forbedring er nøkkelen til å styrke organisasjonens sikkerhetsposisjon over tid.

7.4 Gjenoppretting og rapportering

Etter at trusselen er inneholdt, må du begynne gjenopprettingsprosessen. Dette kan inkludere å gjenopprette data fra sikkerhetskopier, reparere systemer, og sikre at alle sårbarheter som ble utnyttet, er fikset. Det er også viktig å dokumentere hele hendelsesforløpet i en rapport som beskriver hva som skjedde, hvilke tiltak som ble tatt, og hva som kan gjøres for å forhindre lignende hendelser i fremtiden.

7.5 Læring og forbedring

Når en sikkerhetshendelse er håndtert, er det viktig å gjennomføre en grundig gjennomgang for å lære av hendelsen. Dette inkluderer å evaluere hva som fungerte bra, hva som kunne vært gjort bedre, og hvilke nye tiltak som kan implementeres for å forbedre sikkerheten fremover. Læring og kontinuerlig forbedring er nøkkelen til å styrke organisasjonens sikkerhetsposisjon over tid.



8.0 Trender innen IT-sikkerhet.

8.1 Kunstig intelligens og maskinlæring i IT-sikkerhet

Kunstig intelligens (AI) og maskinlæring spiller en stadig viktigere rolle i IT-sikkerhet. Disse teknologiene kan analysere store mengder data for å identifisere mønstre og anomalier som kan indikere et sikkerhetsbrudd. AI kan også brukes til å automatisere responser på visse typer trusler, noe som gir raskere og mer effektiv beskyttelse. Mens AI ikke er en magisk løsning på alle sikkerhetsproblemer, gir det kraftige verktøy som kan styrke sikkerheten din betraktelig.

8.2 Skybasert sikkerhet (cloud security)

Ettersom flere organisasjoner flytter sine data og applikasjoner til skyen, blir sikkerheten i disse miljøene stadig viktigere. Cloud security handler om å beskytte data som er lagret og behandlet i skyen, inkludert gjennom kryptering, tilgangskontroll, og kontinuerlig overvåking. Sikkerhet i skyen krever en annen tilnærming enn tradisjonell IT-sikkerhet, siden du ofte må samarbeide tett med skyleverandørene for å sikre at alle aspekter av miljøet er beskyttet.

8.3 IoT-sikkerhet

IoT-enheter blir stadig mer utbredt, fra smarte termostater og kameraer til industrielle kontrollsystemer. Selv om disse enhetene gir mange fordeler, introduserer de også nye sikkerhetsutfordringer. IoT-enheter er ofte dårlig sikret og kan være enkle mål for hackere. Å sikre IoT-enheter krever spesifikke tiltak, som å endre standardpassord, oppdatere fastvare regelmessig, og segmentere IoT-enheter på egne nettverk.

8.4 Kvantedatamaskiner og kryptering

Kvantedatamaskiner har potensialet til å knekke mange av de krypteringsmetodene som brukes i dag, noe som kan få store konsekvenser for IT-sikkerhet. Forskere jobber allerede med å utvikle kvantesikker kryptering som vil kunne motstå angrep fra kvantedatamaskiner. Mens praktiske kvantedatamaskiner fortsatt ligger noen år frem i tid, er det viktig å være oppmerksom på denne utviklingen og begynne å planlegge for en fremtid hvor kvantesikkerhet blir nødvendig.

8.5 Personvern som en del av sikkerheten (Privacy by Design)

Personvern er en stadig viktigere del av IT-sikkerhet, spesielt med innføringen av lover som GDPR. Privacy by Design innebærer å integrere personvern i utformingen av systemer og prosesser fra starten, i stedet for å legge det til som en ettertanke. Dette inkluderer å minimere datainnsamling, bruke sterke krypteringsmetoder, og sørge for at brukerne har kontroll over sine egne data. Ved å gjøre personvern til en sentral del av sikkerhetsstrategien din, kan du bygge tillit med brukerne og beskytte deres rettigheter.

bravo

+47 24 07 60 60 bravosteps.no hei@bravosteps.no