AVOKI

• En grunnleggende guide i cybersikkerhet

Hva er ett cyberangrep?

AVOKI

Innholdsfortegnelse

AVOKI

● En grunnleggende guide i cybersikkerhet

Digitaliseringens tidsalder

I en verden der digitaliseringen akselererer, blir spørsmål om cybersikkerhet stadig mer relevante. Nesten hver dag møter vi nyheter om cyberangrep på IT-systemer hos bedrifter og myndigheter. Vi blir indirekte berørt av dette, for eksempel når kassasystemer i dagligvarebutikker slutter å fungere, når man ikke kan kjøpe kinobilletter, når netthandel ikke fungerer, og når nettsteder hos bedrifter blir utilgjengelige. Det er snart bare fantasien som setter grenser for hvor sårbart vårt samfunn er!

I takt med at digitaliseringen sprer seg i våre virksomheter ... Men hva ligger egentlig bak disse hendelsene? Hvordan går man frem for å gjennomføre et cyberangrep? I denne guiden vil vi gå gjennom de vanligste elementene i cyberangrep og steg for steg se hvordan man tar seg inn i din datamaskin og nettverk med svært lite tid og ressurser, for deretter å utvide sin tilgang og ta over hele din IT-miljø.

Vi bruker ordet cyberangrep som et samlingsnavn for de ulike metodene som cyberkriminelle – eller hackere – benytter seg av, ofte ved hjelp av en datamaskin og Internett.

Målet med denne guiden er å gi deg, som leser, en overordnet forståelse av hvordan cyberangrep utføres og hvilke tiltak som kan iverksettes for å forhindre dem.

Vårt håp er at etter at du har lest denne guiden, er informert og oppdatert om hvordan et cyberangrep foregår og hvordan du kan handle for å unngå et slikt. Et viktig steg i å beskytte din organisasjon er å stille riktige krav til din IT-leverandør. La oss begynne reisen mot en tryggere digital fremtid.

> **82%**
> av alle inntrengningsforsøk involerer den menneskelige faktoren

- Regulatoriske krav

EU-direktiv – NIS2

EU's NIS2-direktiv tar en sentral rolle i bekjempelsen av cybertrusler. Den 18. oktober 2024 innføres flere krav til virksomhetsledelser gjennom et økt ansvar for å proaktivt identifisere, evaluere og redusere risikoen for cyberangrep. Direktivet gjør det klart at virksomhetsledere personlig er ansvarlige for å kunne håndtere de komplekse og stadig skiftende cybertruslene som eksisterer.

Hvis man ikke lever opp til disse kravene, kan det resultere i betydelige bøter eller sanksjoner. Dette understreker viktigheten av å raskt få virksomhetens cybersikkerhetsstrategi på agendaen og tilpasse strategien til det nye regelverket.

Fra ledelsens side kreves det en høy grad av engasjement og forståelse for å effektivt beskytte virksomheten, noe som innebærer et mer langsiktig ansvar i hvordan man håndterer eksterne cybertrusler. Dette burde plassere etterlevelsen av direktivet øverst på agendaen for bedriftens strategiske planlegging.

- Fremgangsmåten for et cyberangrep

De vanligste metodene for å utføre cyberangrep

Ifølge USA's Cybersikkerhets- og Infrastruktur-sikkerhetsbyrå (CISA) finnes det fem hovedmetoder som cyberkriminelle bruker for å få tilgang til en IT-miljø. Disse inkluderer:

Utnyttende av vanlige applikasjoner

Ved å finne og utnytte sårbarheter i vanlige kontorprogrammer

Bruk av eksterne IT-tjenester

Der tjenester som tilbys av tredjepart utgjør et risikopunkt, for eksempel skylagringstjenester.

Bruk av gyldige kontoer

Ofte gjennom stjålet eller knekt innloggingsinformasjon fra hackede nettsider.

Utnyttelse av tillit

Angriperen får tilgang gjennom et eksisterende forhold, for eksempel en partner som har tilgang til selskapets IT-systemer eller nettverk.

Nettfiske

En svært vanlig teknikk som innebærer å sende villedende e-postmeldinger for å lure mottakere, kalles **phishing** (nettfiske)

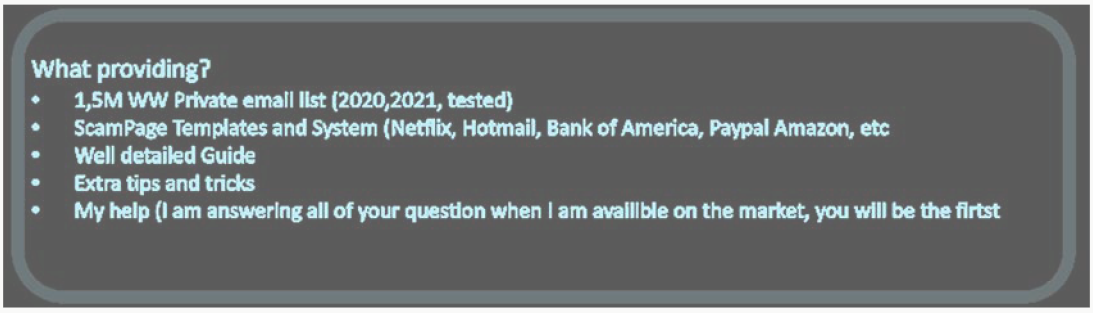
AVOKI

- Den menneskelige faktoren

Social Manipulation

Denne rapporten fra Verizon - *Data Breach Investigation Report* - viser at phishing er den vanligste metoden for innledende cyberangrep, der 82 % av inntrengingene involverer en menneskelig faktor. Av disse er 60 % et resultat av phishing, som for eksempel sosial manipulering (psykologisk manipulasjon av mennesker for å få dem til å utføre handlinger eller avsløre konfidensiell informasjon).
En dyktig hacker kan relativt enkelt lage en skadelig applikasjon som, ved å klikke på en e-postlenke, installerer seg i bakgrunnen på en brukers datamaskin og lager en såkalt bakdør, helt uten at brukeren merker det. Denne bakdøren gir hackeren mulighet til å ta diskret kontroll over systemet.
I dag er det ikke engang nødvendig for cyberkriminelle å gjøre særlig mye for å gjennomføre slike angrep.

På *Dark Web*, en del av internett som krever spesielle programmer for å få tilgang, finnes markedsplasser hvor kriminelle kan kjøpe ferdige phishing-kit.
Disse kitene inneholder alt fra falske e-poster til villedende betalingssider som kan brukes for å stjele informasjon. Kitene, som ofte inkluderer forfalskede betalingssider for kjente merkevarer, er billige og gjør det enkelt å raskt starte en skadelig kampanje. Under er en ekte annonse fra *Dark Web*.
(Slik informasjon er veldig sensitiv og farlig, og det er viktig å være forsiktig når det gjelder nettsider og markedsplasser på det mørke nettet.)



Bilde 1

AVOKI

- Den menneskelige faktoren

Noen av de vanligste metodene

Nedlasting av filer
Skapere av skadelig programvare bruker ofte ulike triks for å få deg til å laste ned skadelige filer. Dette kan være e-postmeldinger med vedlegg eller lenker som ser ut som kvitteringer, betalingsbekreftelser eller fakturaer. Du kan bli bedt om å åpne den vedlagte filen for å fullføre en levering eller motta en betaling.

E-postsvindel
E-post er i dag et arbeidsverktøy som brukes i organisasjoner over hele verden, men det er også en angrepsvektor for cyberkriminelle. Noen skadelige e-poster er enkle å identifisere på grunn av dårlig stavemåte eller ukjente avsendere. I dag bruker cyberkriminelle generativ AI for å lage troverdige, perfekt utformede og profesjonelt laget meldinger som sendes til tusenvis av mottakere via e-post. Det er også vanlig at disse e-postene forfalskes for å se ut som de kommer fra et kjent og pålitelig selskap eller en kjent person. Skadelig programvare kan også hacke e-postkontoer og bruke dem til å sende spam til hele kontaktlisten.
Ifølge Deloitte starter 91 prosent av alle cyberangrep via e-post, der skadelige lenker og vedlegg benyttes for å åpne bakdører for cyberkriminelle.

Microsoft Office-filer
Microsoft Office, som er en velkjent programvaresuite for produktivitet, inneholder et kraftig skriptspråk for programmering, som gir brukere muligheten til å lage avanserte funksjoner. Dette skriptspråket kan imidlertid misbrukes av kriminelle for å utvikle skadelige skript som installerer skadelig kode eller utfører andre skadelige aktiviteter. Vanligvis vil du få en advarsel når du åpner slike filer.

Flyttbare lagringsenheter
En annen metode for spredning av skadelig programvare er gjennom flyttbare lagringsenheter som USB-minner og eksterne harddisker. Når disse infiserte enhetene kobles til datamaskinen din, kan den skadelige programvaren installeres automatisk.

Installasjon av applikasjoner
Noen ganger kan skadelig programvare snike seg inn i systemet ditt sammen med andre programmer du laster ned, spesielt fra nettsteder som ikke er fra de offisielle leverandørene av applikasjonene, eller via filer delt i private P2P-nettverk (peer-to-peer).

Websites og nettlesere
Besøk på visse nettsteder kan føre til cyberangrep, enten fordi nettstedet i seg selv er skadelig, eller fordi den legitime siden har blitt hacket. Disse angrepene utnytter sårbarheter i nettleseren din. Derfor er det svært viktig å alltid oppdatere all programvare til den nyeste versjonen, spesielt nettleseren, og å fjerne ubrukte nettlesertillegg.

Å forstå disse metodene er et viktig steg for å beskytte datamaskinen og dine personlige data mot cybertrusler. Regelmessige oppdateringer, forsiktighet med nedlastinger og e-postmeldinger, samt sikker håndtering av flyttbare enheter og applikasjoner, er grunnleggende for et effektivt vern.

Hvordan foregår et cyberangrep?

De ulike fasene

For å belyse hvordan en av de vanligste inntrengene kan foregå og hvordan det utføres, vil vi her gå gjennom de forskjellige fasene av et vanlig angrep og hvordan en hacker kan infiltrere din datamaskin og IT-miljø.

For å gi innsikt i hvordan et angrep skjer, vil vi nedenfor forklare hvordan et av de vanligste cyberangrepene foregår, og hvordan hackere tar seg inn i din datamaskin og IT-miljø.

Fase 1: Phishing-angrepet

Et vanlig første steg for en hacker er å utføre et phishing-angrep. Dette innebærer ofte å sende e-poster som ser "ekte" ut, komplett med fristende tilbud eller oppfordringer som vekker mottakerens nysgjerrighet. Når mottakeren klikker på en lenke eller vedlegg i meldingen, aktiveres et lite program som uten mottakerens viten starter flere prosesser på datamaskinen og skaper en bakdør til brukerens datamaskin. Innen noen sekunder etter klikket etableres permanent tilgang for hackeren.

Fase 2: Utforske det interne IT-miljøet

Når hackeren først har tilgang til datamaskinen og er inne i systemet, bruker de brukerens rettigheter for å søke etter andre datamaskiner i nettverket. Dette kan innebære å bruke ulike digitale verktøy for å lete etter delte filer, applikasjonsdatamaskiner, database- og webservere, og noen ganger også skriverens webgrensesnitt, som kan gi verdifull informasjon for videre inntrengning.

Fase 3: Utnyttelse av skriveren

Skrivere er ofte sårbare punkter som blir oversett. Hackeren kan utnytte svakheter i skriverens sikkerhet, som standardpassord eller ingen passord i det hele tatt, for å få tilgang til høyere rettigheter. De kan bla gjennom skriverens webapplikasjon og få tilgang til konfigurasjonsinnstillinger.

Ved å manipulere innstillingene på skriveren kan hackeren interagere med andre systemer i nettverket og ved hjelp av digitale verktøy fange opp e-postadresser, passord og brukerkontoer samt annen informasjon om nettverket som kan være verdifull for videre inntrengning.

Standardinnstillingene for mange skrivere er å tillate tilgang til webapplikasjonen uten passord, og hvis det finnes et passord, glemmer mange brukere å endre standardpassordet, som lett kan finnes i brukermanualer på nettet. Hvis en hacker får tilgang til en skriver som har funksjonen til å skanne dokumenter og sende dem som e-poster, kan dette utnyttes til ondsinnede formål.

For å kunne sende e-poster, er kanskje skriveren konfigurert med en brukerkonto som har høyere rettigheter enn en gjennomsnittlig bruker. Hackere som har digitale verktøy for å finne passordet til denne kontoen, kan deretter misbruke det for å utføre ytterligere inntrengning i nettverket eller for å samle inn konfidensiell informasjon.

Fase 4: Utvidet tilgang

Med tilgang til høyere rettigheter begynner hackeren å utforske IT-miljøet grundigere. Dette kan innebære å søke gjennom filer og sensitiv informasjon, og finne administrator-kontoer som kan brukes til å få full kontroll over IT-miljøet.

Systematisk og metodisk leter hackeren gjennom all informasjon han kan få tilgang til, og før eller senere finner han opplysninger, og ikke sjelden et administratorkonto med tilhørende passord, gjemt et sted i gamle sikkerhetskopier eller gamle delinger.

Mangelen på oversikt over det nåværende IT-miljøet og hva tidligere IT-administratorer har opprettet og aldri ryddet ut, gjør at man blir sårbar for cyberangrep. Ved hjelp av det stjålne passordet for administratoren får hackeren nå full tilgang til hele IT-miljøet, filer, kontoer, økonomiske opplysninger og mye, mye mer...

Fase 5: Fullstendig overtakelse

I det siste steget har hackeren full kontroll over IT-miljøet og kan gjøre hva han eller hun vil. Denne tilgangen kan brukes til å kryptere informasjon i et såkalt ransomware-angrep, som tvinger selskapet til å betale en løsesum for å få tilbake tilgangen til sine data.
Hackeren kan også bruke IT-ressurser fra IT-miljøet til å spre eller dele ulovlig informasjon på internett samt spre skadelig programvare.
Ved å ha full tilgang til hele IT-miljøet og datamaskinen som kontrollerer sikkerheten, kan hackeren gjøre stort sett hva han eller hun vil, for eksempel bruke et verktøy for å laste ned alle bruker- og kontoopplysninger, og alle krypterte passord kan knekkes av et verktøy som gjør milliarder av gjetninger på noen sekunder.

Nå har hackeren full tilgang og kan logge inn med administrativ tilgang til hele organisasjonen og kryptere hele eller deler av IT-miljøet.
Dette viser hvor sofistikerte og skadelige cyberangrep kan være, og understreker viktigheten av proaktive sikkerhetstiltak for å beskytte ditt IT-miljø.

● Hvordan beskytter jeg meg?

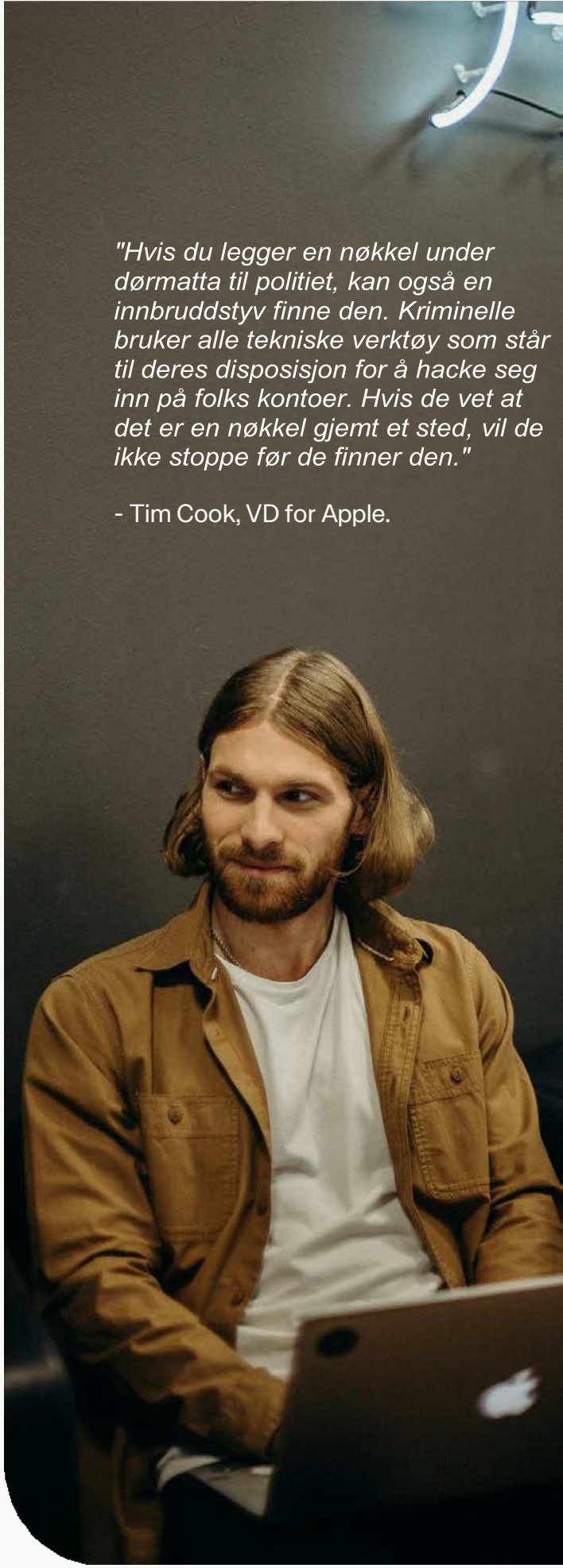
Hva kan jeg gjøre for å forebygge?

Å beskytte ditt IT-miljø mot cyberangrep er en av de mest kritiske utfordringene organisasjoner står overfor i dagens digitale tidsalder.

Med cybertrusler som stadig øker i antall, blir det stadig viktigere å implementere robuste sikkerhetstiltak for å beskytte sensitiv informasjon. En effektiv strategi inkluderer bruken av avansert teknologi, som brannmurer og antivirusprogrammer, som spiller en nøkkelrolle i å identifisere og avverge potensielle trusler.

Kontinuerlig overvåking av nettverket er avgjørende for raskt å oppdage og handle på mistenkelige aktiviteter. Det er også viktig å ikke undervurdere verdien av å utdanne brukerne. Ved å informere brukerne om de siste cybertruslene og hvordan man unngår dem, kan mange sikkerhetshendelser forhindres allerede fra starten.

En kombinasjon av disse metodene gir et sterkt fundament for å effektivt beskytte sensitiv informasjon og minimere risikoen for datainnbrudd og andre sikkerhetsrelaterte hendelser.
Nedenfor er noen av de ulike systemene og løsningene samt tiltakene som finnes for å sikre en organisasjons cybersikkerhet. Selvfølgelig er størrelsen på virksomheten relevant for hvilken type system eller løsning man anser seg å ha råd til, men å begynne å se seg rundt og reflektere over sitt vern mot cybertrusler er relevant for alle.



System og løsninger

Microsoft 365
Microsoft 365 tilbyr omfattende sikkerhet for å forebygge, oppdage og håndtere cybertrusler. Denne beskyttelsen inkluderer avanserte anti-phishing-funksjoner i Microsoft Defender som advarer om potensielle e-postsvindel og uvanlige tegn i avsenderadresser.
Microsoft Defender for Office 365 fungerer som en enhetlig sikkerhetsplattform som automatisk oppdager skadelig og mistenkelig innhold på tvers av flere applikasjoner, inkludert e-post og Microsoft Teams.
OneDrive for Business tilbyr beskyttelse mot ransomware-angrep ved å tillate gjenoppretting av tidligere versjoner av filer. Disse sikkerhetsfunksjonene er avgjørende for å beskytte organisasjoner mot et mangfold av cybertrusler.

Nettverkssegmentering
Nettverkssegmentering er en effektiv strategi for å forbedre cybersikkerheten innen en organisasjon. Denne metoden innebærer å dele opp et nettverk i mindre deler eller segmenter. Ved å gjøre dette kan man effektivt begrense skaden ved et cybersikkerhetsangrep, da en angriper som lykkes med å trenge inn i en del av nettverket, vil ha vanskeligheter med å spre seg til andre deler. Hvert segment i et nettverk kan ha egne sikkerhetsregler og tilgangskontroller. Dette gjør det mulig å skreddersy sikkerhetsnivået for hver del av nettverket avhengig av dens sensitivitet og behov.

Uansett hvordan hackere får tilgang til datamaskinen din, er nettverkssegmentering en enkel, men svært effektiv måte å begrense hvor mye av nettverket ditt en hacker kan få tilgang til dersom de kommer inn i miljøet ditt.

Installere EDR- og XDR-teknologi
EDR- (Endpoint Detection and Response) og XDR-teknologi (Extended Detection and Response) systemer overvåker mye mer enn tradisjonelle antivirusbeskyttelser og tilbyr sofistikerte funksjoner for å beskytte mot cybertrusler.

EDR-teknologien fokuserer på å overvåke og beskytte individuelle enheter som datamaskiner, servere og mobile enheter.
Systemet overvåker kontinuerlig hver enhet i sanntid, samler inn og analyserer data for å identifisere og reagere på mistenkelig atferd og skadelig aktivitet. Det gjør det raskt å finne og håndtere mistenkelige aktiviteter samt stoppe sikkerhetshendelser.

XDR-teknologien omfatter et større perspektiv på cybersikkerhet ved å integrere innsamling, overføring og måling fra datamaskiner, mobiltelefoner, nettverk og skyløsninger. XDRs evne til å samle inn, finne sammenhenger og analysere data fra ulike sikkerhetslag gir mulighet for raskere oppdagelse og respons på avanserte cybertrusler. Systemet tilbyr sentralisert synlighet av sikkerhetssituasjonen og automatisering av ulike forebyggende sikkerhetstiltak.

Hver organisasjon bør vurdere å bruke EDR og XDR. Begge teknologiene er nødvendige for å utvikle en effektiv cybersikkerhetsstrategi. Begge bruker tilpasset deteksjon av cybertrusler og AI-teknologi for automatisk å gjenkjenne og svare på trusler før de kan skade organisasjonen.

AVOKI

91%

Av alle cyberangrep begynner via e-post, der skadelige lenker og vedlagte filer brukes for å åpne bakdører for cyberkriminelle.

Kilde: Deloitte

Bruk prinsippet om minst mulige privilegium

Å implementere prinsippet om minst mulige privilegium er en grunnleggende del av en effektiv cybersikkerhetsstrategi.
Dette prinsippet innebærer at hver bruker, prosess eller program kun får tilgang til de ressurser og privilegier som er absolutt nødvendige for å utføre sine tildelte oppgaver eller funksjoner. Ved å begrense tilgangen til kun det nødvendige, reduseres risikoen for utilsiktede eller bevisste datainnbrudd og cyberangrep.

For å implementere dette effektivt bør organisasjoner gjennomføre en grundig analyse av brukerroller og deres tilgangsbehov for å fastsette passende tilgangsnivå for hver bruker eller rolle. Prinsippet om minst mulige privilegium er en hjørnestein i en Zero Trust-sikkerhetsmodell, hvor hver tilgangsbegjæring verifiseres og valideres, uavhengig av hvor den kommer fra.

AVOKI

Styrk og begrens tilgang til kritisk systemkonfigurasjon.

Å styrke og begrense tilgangen til kritisk systemkonfigurasjon er et viktig steg for å forbedre cybersikkerheten.
Dette innebærer å iverksette flere tiltak for å redusere risikoen for uautorisert tilgang og beskytte sensitiv informasjon.

1. Krev sterk autentisering
Bruk sterke autentiseringsmetoder, som multifaktorautentisering (MFA), for å beskytte webgrensesnitt og andre kritiske systemer. Dette er spesielt viktig for tjenester som er tilgjengelige eksternt, som VPN-tjenester.

2. Deaktiver unødvendige tjenester og segmenter nettverket
Det er viktig å deaktivere tjenester som ikke er nødvendige og segmentere nettverket for å begrense tilgang til kritiske systemer. Ved å dele nettverket opp i mindre deler, kan du lage unike sikkerhetspolicyer og kontroller for hvert segment, noe som effektivt hindrer angripere fra å bevege seg fritt i nettverket.

3. Rutinemessige oppdateringer av programvare
Kontinuerlige oppdateringer og forbedringer av programvare er nødvendige for å beskytte mot kjente sårbarheter. Regelmessig installasjon av sikkerhetsoppdateringer hjelper med å tette sikkerhetshull som angripere kan utnytte.

1. **Begrens fysisk tilgang til nettverksporter**
   Det er viktig å begrense fysisk tilgang til nettverksporter for å hindre uautorisert tilgang og potensielle innbrudd.

2. **Bruke fil- og enhetskryptering**
   Kryptering av data, både i ro og under overføring, beskytter sensitiv informasjon fra å bli lest av uautoriserte.

3. **Installer og brusikkerhetsprogramvare**
   Det er viktig å ha oppdatert sikkerhetsprogramvare, som antivirus og brannmurer, for å beskytte mot ulike typer cyberangrep.

4. **Logging og overvåkning**
   Implementer loggings- og overvåkingsverktøy for å kunne spore og analysere mistenkelig aktivitet i systemet.
   Gjennom å implementere noen av disse tiltakene kan organisasjoner skape et mer sikkert og motstandsdyktig IT-miljø som er bedre rustet til å motstå og reagere på cybertrusler.

Bruk multifaktorautentisering

Bruken av multifaktorautentisering (MFA) er en viktig strategi for å styrke cybersikkerheten.

MFA benytter en flerskiktsmetode for å sikre data og applikasjoner ved å kreve at brukeren presenterer en kombinasjon av to eller flere autentiseringsfaktorer for å verifisere sin identitet ved pålogging. Dette øker sikkerheten betydelig, fordi selv om en autentiseringsfaktor, som et passord, blir kjent for en hacker, vil en uautorisert bruker ikke kunne oppfylle det andre autentiseringskravet og dermed ikke få tilgang til det fysiske området, enheten, nettverket eller IT-miljøet.
MFA er spesielt effektivt for å beskytte mot ulike typer cyberangrep, inkludert phishing, sosial manipulasjon og gjetteangrep på passord. Det beskytter også mot innlogginger fra angripere som utnytter svak eller stjålet informasjon.

De tre vanlige autentiseringsfaktorene som brukes i MFA er noe du kjenner til (f.eks. et passord eller en PIN-kode), noe du har (f.eks. en smarttelefon eller en sikkerhetstoken), og noe du er (f.eks. biometriske data som fingeravtrykk eller ansiktsgjenkjenning).
Ved å kreve bevis fra to eller flere av disse kategoriene, skapes en sterkere sikkerhetsbarriere.
Det er viktig å anvende MFA i din organisasjon, ikke bare for eksterne servere, men også for intern administratoradgang. Ved å begrense tilgangen til kritiske systemer med MFA kan du effektivt redusere risikoen for at hackere får tilgang til sensitiv informasjon eller kritiske systemer.

Gjennomfør penetrationstester

Penetrasjonstester, utført av etiske hackere, er en svært effektiv metode for å identifisere og håndtere svakheter i et selskaps IT-infrastruktur. Denne prosessen innebærer et simulert cyberangrep for å finne sårbarheter i nettverk og systemer. Ved proaktivt å identifisere svakheter som kan utnyttes av hackere, kan et selskap redusere risikoen for vellykkede datainnbrudd eller hendelser.

Penetrasjonstester gir en objektiv vurdering av systemets sikkerhetskontroller og oppdager ofte alvorlige sårbarheter som kan ha blitt oversett av automatiserte skanninger. Penetrasjonstester kan kategoriseres i forskjellige tilnærminger som gir ulike innsikter avhengig av den kunnskapen den etiske hackeren har om systemet.
Testene er ikke bare en teknisk kontroll, men en prosess som må utvikles og kontinuerlig forbedres over tid.

Penetrasjonstester er nødvendige for en moden cybersikkerhetsstrategi og bør ikke overses av selskaper som ønsker å beskytte sin kritiske infrastruktur mot cybertrusler.

Microsoft Secure Score

Microsoft Secure Score er et verktøy for å måle en organisasjons sikkerhetsstatus, og resultatet sammenlignes med bransjestandarder og Microsofts sikkerhetsanbefalinger. En høyere poengsum indikerer bedre sikkerhet, og poengsummen hjelper til med å måle fremgang over tid. Verktøyet gir anbefalinger for å forbedre organisasjonens sikkerhet, med fokus på å identifisere og adressere svakheter i områder som kan forbedres. Verktøyet hjelper til med å vurdere sikkerheten på tvers av ulike områder som identitet, enheter, informasjon, applikasjoner og infrastruktur.

> Opptil 70 % reduseres risikoen for cyberangrep ved å utdanne sine brukere.
>
> Kilde: Aberdeen Group

Ved å sammenligne organisasjonens status over tid og med andre organisasjoner kan man lage en plan for å forbedre sikkerheten.

Microsoft Secure Score-poengene kan brukes som grunnlag for rapportering av det nåværende sikkerhetsnivået og forbedringer til ledelsen, samt danne grunnlag for endringer i sikkerhetsstrategien. Verktøyet er integrert med andre Microsoft-produkter og kan også ta hensyn til når en tredjepartsløsning har blitt brukt for å håndtere anbefalte tiltak. Dette gjør det mulig å tydeliggjøre fremdriften som gjøres for å bedre beskytte organisasjonens IT-miljø.

Opplæring av brukere i cybersikkerhet

Til tross for at maskinvare- og programvarebeskyttelse er viktige aspekter av cybersikkerhet, kan de ikke alene fange opp alle phishing-angrep. Ifølge en studie fra Aberdeen Group kan opplæring i sikkerhetsbevissthet redusere risikoene med 45–70 %, noe som fremhever viktigheten av regelmessig og effektiv opplæring for å øke bevisstheten om cybersikkerhet blant brukere.

En annen studie fra Proofpoint viste at selskaper som implementerte opplæring i sikkerhetsbevissthet så en reduksjon på opptil 40 % i antallet skadelige lenker som ble klikket på av brukere.

Dette understreker viktigheten av å kontinuerlig minne brukerne om risikoene, samt investere i månedlig opplæring eller informasjon om cybersikkerhet for ansatte.

Brannmur

En brannmur er en avgjørende komponent i et organisasjons nettverkssikkerhet og fungerer som en barriere for å beskytte nettverk mot uautorisert tilgang og cybertrusler. Den kan være enten en fysisk enhet (maskinvarebrannmur) eller et program (programvarebrannmur) og er designet for å overvåke og kontrollere innkommende og utgående nettverkstrafikk basert på et sett med forhåndsdefinerte sikkerhetsregler.

Brannmurer plasseres ofte mellom Internett og et privat nettverk, vanligvis i tilknytning til eller integrert i en ruter. Disse overvåker trafikken mellom nettverkene og bruker sikkerhetsregler for å hindre uønsket eller skadelig trafikk fra å nå de interne systemene. Det finnes programvarebrannmurer som installeres direkte på datamaskiner eller enheter for å gi beskyttelse på individuell nivå.

En brannmurs hovedoppgave er å filtrere nettverkstrafikk og blokkere uautoriserte forsøk på å få tilgang til et system eller nettverk. Dette inkluderer å hindre visse typer phishing-angrep og andre cybertrusler.

Men brannmurer har begrensninger, spesielt når det gjelder mer sofistikerte phishing-angrep som er rettet direkte mot brukere for å få dem til å avsløre sensitiv informasjon. Regelmessig gjennomgang og oppdatering av brannmurregler og konfigurasjoner er avgjørende for å opprettholde effektiv nettverkssikkerhet.

Backup – Sikkerhetskopiering

Å implementere en strategi for sikkerhetskopiering som inkluderer flere generasjoner av sikkerhetskopier er en kritisk komponent i en robust cybersikkerhetsstrategi. Cybertrusler som ransomware (utpressing) og virus utgjør alvorlige risikoer mot dataintegritet, og her fungerer sikkerhetskopiene som et avgjørende sikkerhetstiltak for å beskytte organisasjonens verdifulle informasjon.

Når et cyberangrep inntreffer, kan konsekvensene være katastrofale, enten ved at kritisk informasjon blir låst eller ødelagt. Ved å ha en sikkerhetskopi, altså en backup, kan organisasjonen effektivt gjenopprette sin digitale informasjon fra et punkt før angrepet. Dette er spesielt verdifullt i tilfeller der den nyeste sikkerhetskopien også er utsatt.

Å ha en strategi for flere generasjoner av sikkerhetskopier er ikke bare en forsikring mot datatap på grunn av cyberangrep, men også en avgjørende komponent for å opprettholde forretningskontinuitet og operasjonell stabilitet. Dette er et svært viktig tiltak som sikrer at organisasjonens digitale eiendeler forblir beskyttet og tilgjengelige, selv i en verden med stadig mer sofistikerte cybertrusler.

> Effektene av et cyberangrep kan få store konsekvenser for samfunnsviktige funksjoner og kritiske IT-systemer, og de direkte og indirekte kostnadene for cyberangrep beregnes å beløpe seg til milliardbeløp. Kilde: SÄPO - Säkerhetspolisen

● Vårt unike tilbud

Hvordan vår løsning beskytter mot cybertrusler

Som et svar på den kompleksiteten som råder innen cybersikkerhet, har vi utviklet to tjenester som sammen benytter Microsofts XDR-løsning (Extended Detection and Response). Denne løsningen gir omfattende beskyttelse ved å integrere og analysere data fra hele organisasjonens IT-miljø, og identifisere trusler i sanntid.

Microsoft XDR er et sikkerhetssystem som gir et helhetlig og integrert bilde av sikkerhetstrusler på tvers av hele organisasjonens IT-miljø. Dette inkluderer nettverk, enheter, applikasjoner og skytjenester. Ved å kombinere Microsoft XDR med vår egen ekspertise, har vi tatt overvåkningen av cyberangrep et steg videre.

Med hjelp av kunstig intelligens (AI) og avanserte rapport- og analyseverktøy, overvåkes din IT-miljø kontinuerlig. Dette gjør det mulig å identifisere og reagere på trusler i sanntid, samtidig som det gir en detaljert innsikt i sikkerhetsstatusen og potensielle risikoer i systemene dine.

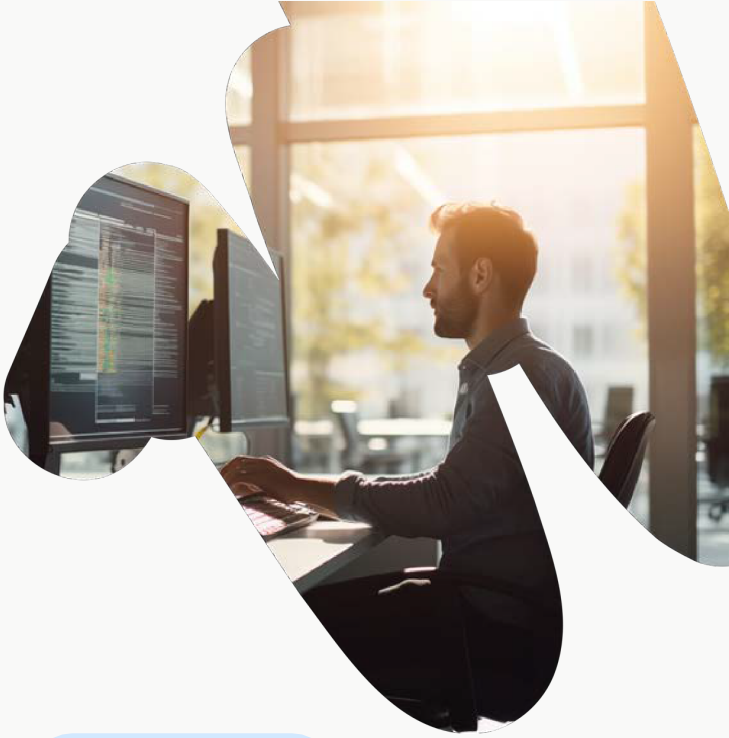
Microsoft XDR tilbyr en rekke funksjoner, men det kan oppleves som ganske vanskelig å navigere for vanlige brukere. Det er mange innstillinger som kan gjøres, og noen ganger er det usikkert hva alle innstillingene gjør eller hva de er til for.

Vår tjeneste tilbyr en effektiv løsning på dette, og vi har utviklet to tjenester som vi tilbyr våre kunder. Vi tar oss av innstillingene i deres Microsoft-miljø basert på deres unike behov og bruksmønstre.

AVOKI

● Vårt unike tilbud

X-One Cloud Security



Med denne unike løsningen garanterer vi ikke bare skreddersydd sikkerhet basert på ditt selskaps spesifikke behov, men også en automatisk overvåking som holder brukerne og dataene dine beskyttet.

X-ONE 365 Cloud Security kombinerar

Sikkerhet med hjelp av Kunstig Intelligens: Apex Insight

Vår egenutviklede overvåkingsagent sikrer ditt selskap og brukere ved hjelp av Kunstig Intelligens.
Med avanserte algoritmer identifiserer Apex Insight risikofylte og trusselaktige atferdsmønstre og blokkerer brukerkontoer. Når en satt risikogrense eller trusselterskel er passert, varsler X-ONE Cloud Security en sikkerhetsspesialist, og dere som kunde mottar etter analyse en forensisk rapport om hva som har skjedd.

Analys av digitala användarmönster och beteenden för ditt företag

Säkerställer din företagsintegritet och beteendemönster genom att granska inloggningsdata samt skapa villkorliga åtkomstregler. Beroende på hur man sätter upp säkerhetsnivån kan man tillåta, begränsa eller blockera åtkomst. Blockeringsregler uppdateras dynamiskt med aktuell omvärldsinformation.

Övervakning av tjänsternas hälsostatus med Tennant Health

Vi övervakar status på Microsoft-molntjänster, inklusive Office på webben, Microsoft Teams, Exchange Online och Microsoft Dynamics 365. Om det är problem med en molntjänst meddelar vi er och kan avgöra om det är ett känt problem med en pågående lösning, allt detta innan du ringer support eller spenderar tid på felsökning.

Detaljerte kvartalsinnsikter, skreddersydd for IT og beslutningstakere
Vi leverer kontinuerlige analyser, oppdateringer og justeringer i lys av nye trusler og retningslinjer. Dette for at du som kunde skal kunne føle deg trygg på at beskyttelsen fungerer, samt ha et grunnlag for beslutninger om eventuelle endringer på grunn av økt trusselbilde eller oppdatering av IT-policy for tilgang til selskapets IT-miljø.

X-One Endpoint Security / Premium

X-ONE 365 Endpoint Security (EDR) er en avansert sikkerhetstjeneste som bygger på Microsoft XDR og gir virksomheter et nytt nivå av proaktivt beskyttelse. Gjennom omfattende overvåkning og respons, samt effektiv håndtering av digitale enheter som datamaskiner, mobiltelefoner og nettbrett, kan du føle deg trygg. Tjenesten gir organisasjoner muligheten til å raskt identifisere, håndtere og adressere sikkerhetstrusler i sanntid, noe som reduserer risikoen for innbrudd og sikrer kontinuerlig beskyttelse for alle enheter i nettverket.

Med detaljerte sikkerhetsrapporter og integrasjon med Microsoft Defender for Endpoint, tilbyr denne tjenesten en omfattende beskyttelsesmekanisme for deres IT-systemer. **X-ONE 365 Endpoint Security** gir en kontinuerlig oppdatert, proaktiv sikkerhetsløsning som effektivt håndterer og responderer på trusler, slik at organisasjonen kan opprettholde et høyt sikkerhetsnivå og redusere risikoen for cyberangrep.

Proaktiv beskyttelse

Sikre enhetene dine med et proaktivt beskyttelsessystem.

Overvåkning

Kontinuerlig overvåkning av skadelige aktiviteter på enheter.

Insikter

Detaljerte kvartalsinnsikter, skreddersydd for IT og beslutningstakere.

Sofistikert overvåkning

Ved å overvåke Microsoft Defender, identifiserer X-ONE 365 Endpoint Security datamaskiner med risikofylte atferdsmønstre og potensielle virus, samtidig som det sikres en proaktiv beskyttelsesmetode.

Automatiska alarm

Når tjenesten oppdager en risiko eller trussel, utløses en automatisk alarm som varsler sikkerhetsteknikere, som deretter kan iverksette nødvendige tiltak. Når tjenesten oppdager en risiko, varsles den ansvarlige teknikeren og den utsatte enheten isoleres automatisk for å redusere risikoen for spredning.

Med tilleggstjenesten **Endpoint Security Premium** legges flere automatiske tiltak til for å redusere spredning, inkludert isolering og deaktivering av enheter, samt SMS-varsler til de ansvarlige personene.

Defender Endpoint Hardening

Ved implementering av X-ONE 365 Endpoint Security utføres en analyse basert på Microsofts **Exposure Score** samt Xites egen ekspertise. Basert på denne analysen defineres de nødvendige reglene for å sikre en trygg og funksjonell klient/server-miljø.

Arbeidet med å sikre miljøet er en kontinuerlig prosess. Analyse og justering av innstillinger er en del av den pågående prosessen som inngår i X-ONE 365 Endpoint Secuity. Når nye trusler og retningslinjer publiseres, oppdaterer vi også miljøet deres i tråd med disse forutsetningene.

Forensisk Analyse

For hvert bekreftet trussel, gjennomføres en grundig forensisk analyse. En detaljert rapport sendes til kunden, som inneholder viktig informasjon som datamaskinnavn, tidspunkt for risikofinning, type risiko og alvorlighetsgrad, samt datamaskinens status

Kvartalsrapporter

Hver kvartal mottar du en rapport med utfyllende informasjon om sikkerheten i deres miljø. Denne rapporten inkluderer selskapets eksponeringsscore, eventuelle sårbarheter i operativsystemer og applikasjoner, samt detaljert informasjon om klient- og servermiljøer.

● Avslutningsvis

Digitaliseringens tidsalder

Avslutningsvis er det viktig å påpeke at som bedrift bør man være bevisst på viktigheten av å beskytte sin IT-miljø mot cyberangrep.

Det er avgjørende å implementere robuste sikkerhetstiltak. Gjennomgå beskyttelsen deres i dag, og vurder å begynne å bruke avansert teknologi som EDR- og XDR-teknologi dersom det ikke allerede er en del av IT-miljøet deres.

Husk at regelmessig opplæring i sikkerhetsbevissthet og penetrasjonstester er viktige for å minimere risiko og oppdage svakheter før hackerne gjør det. Mentaliteten om at «det rammer andre, ikke meg» må utfordres. Det er ikke et spørsmål om *om* du blir rammet, men *når*. Sørg for at du er beskyttet før det er for sent.