AVOKI

• En grundläggande guide i cybersäkerhet

Vad är ett cyberangrepp?

AVOKI

Innehåll

Vad är ett cyberangrepp?	3
Regulatoriska krav – NIS2	4
Tillvägagångsätt för ett cyberangrepp	5
Den mänskliga faktorn	6
Vanliga metoder för cyberangrepp	7
Hur går et cyberangrepp till?	8
Hur skyddar jag mig?	12
Vårt unika erbjudande	19
Avslutningsvis	23

● En grundläggande guide i cybersäkerhet

Digitaliseringens tidsålder

I en värld där digitaliseringen accelererar, blir frågor om cybersäkerhet alltmer relevanta. Nästan varje dag stöter vi på nyheter om cyberangrepp i IT-system hos företag och myndigheter. Vi blir indirekt drabbade av att till exempel kassasystem hos livsmedelskedjor är ur funktion, att man inte kan köpa biobiljetter, e-handel som inte fungerar och webbsidor hos företag som är onåbara. Det är snart bara fantasin som sätter gränser för hur sårbart vårt samhälle är i takt med att digitaliseringen breder ut sig i våra verksamheter.

Men vad ligger egentligen bakom dessa incidenter?

Hur går man tillväga för att genomföra ett cyberangrepp?

I den här guiden kommer vi att gå igenom de vanligaste orsakerna till cyberangrepp och steg för steg se hur man tar sig in i din dator och nätverk med mycket lite tid och resurser, för att sedan utöka sin åtkomst och ta över hela din IT-miljö.

Vi använder ordet cyberangrepp som ett samlingsnamn för de olika metoderna som cyberbrottslingar – eller hackare - använder sig av, oftast med hjälp av en dator och Internet. Målet med denna guide är att ge dig, som läsare en övergripande förståelse av hur cyberangrepp utförs och vilka åtgärder som kan vidtas för att förhindra dem.

Vår förhoppning är att efter att du läst denna guide är informerad och uppdaterad över hur ett cyberangrepp går till och hur du kan agera för att undvika en sådan.

Ett viktigt steg i att skydda din organisation är att ställa rätt krav på din IT-leverantör. Låt oss börja resan mot en säkrare digital framtid.

82%

av alla intrångsförsök involverar den mänskliga faktorn

- Regulatoriska krav

EU-direktiv – NIS2

EU:s NIS2-direktiv tar en central roll i bekämpningen av cyberhot. Den 18 oktober 2024, intensifieras kraven på verksamhetsledningar genom ett ökat ansvar för att proaktivt identifiera, utvärdera och reducera risken för cyberangrepp. Direktivet gör klart att verksamhetsledare personligen ansvarar för att kunna hantera de komplexa och ständigt föränderliga cyberhot som existerar.

Lever man inte upp till dessa krav kan det resultera i avsevärda böter eller sanktioner. Detta om något understryker vikten av att snabbt få upp verksamheters cybersäkerhetsstrategi på agendan och att anpassa strategin till det nya regelverket.

Från ledningens sida krävs en hög grad av engagemang och förståelse för att effektivt skydda verksamheten, vilket innebär att man står inför ett mer långtgående ansvar i hur man hanterar externa cyberhot. Det borde placera efterlevnaden av direktivet högst upp på agendan för företags strategiska planering.

● Tillvägagångsätt för ett cyberangrepp

De mest vanligaste metoderna att utföra attacker

Enligt USA:s Cybersäkerhets- och Infrastruktursäkerhetsbyrå (CISA) finns det fem huvudsakliga metoder som cyberbrottslingar använder för att initialt få tillgång till en IT-miljö. Dessa inkluderar:

Utnyttjande av allmänna applikationer

Genom att hitta och använda sårbarheter i vanliga kontors-programvaror

Användning av externa IT-tjänster

Där tjänster som erbjuds av tredje part utgör en riskpunkt, t.ex. Molntjänster

Användning av giltiga konton

Ofta genom stulen eller knäckt inloggnings-information från hackade internetsajter

Utnyttjande av förtroende

Angriparen tar sig in genom en befintlig relation t.ex. en partner som har tillgång till företagets IT-system eller nätverk.

Nätfiske

En mycket vanlig teknik som innebär att skicka vilseledande e-post-meddelanden för att lura mottagare

- Den mänskliga faktorn

Social Manipulation

En rapport från Verizon - Data Breach Investigation, påvisar att nätfiske är den vanligaste metoden för initiala cyberangrepp, där 82% av intrången innefattar en mänsklig faktor.
Av dessa är 60% ett resultat av nätfiske, som till exempel social manipulation (psykologisk manipulation av människor så att de utför handlingar eller avslöjar konfidentiell information) för att få människor att avslöja känslig information.

En skicklig hacker kan relativt enkelt skapa en skadlig applikation som, genom ett klick på en e-postlänk, installerar sig självt i bakgrunden av en användares dator och skapar en så kallad bakdörr helt obemärkt för dig som användare. Denna bakdörr möjliggör för hackaren att diskret ta kontroll över systemet.

Det är idag inte ens nödvändigt för cyberbrottslingar att anstränga sig särskilt mycket i dessa attacker.

På ”Dark Web”, en del av internet som kräver speciella program för tillgång, finns marknadsplatser där brottslingar kan köpa färdiga kit för nätfiske.

Dessa kit innehåller allt från falska e-postmeddelanden till vilseledande betalningssidor som kan användas för att stjäla information.

Dessa kit, som ofta inkluderar förfalskade betalningssidor för välkända varumärken, är billiga och gör det enkelt att snabbt starta en skadlig kampanj. Nedan är en verklig annons från Dark Web. (bild 1)

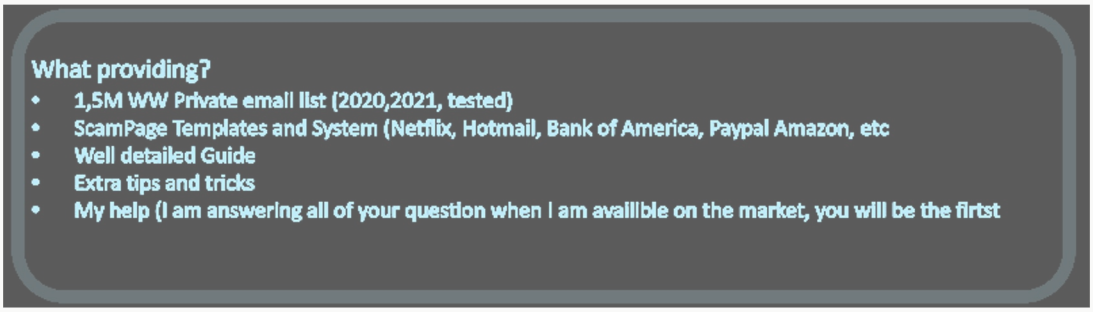

Bild 1

- Den mänskliga faktorn

Några av de vanligaste metoderna

Nedladdning av fil
Skapare av skadlig kod använder ofta knep för att få dig att ladda ner skadliga filer. Det kan handla om ett e-postmeddelande med en bilaga eller en länk som verkar vara ett kvitto, en betalningsbekräftelse eller en faktura. Du kan bli ombedd att öppna den bifogade filen för att slutföra en leverans eller för att motta en betalning.

E-postbedrägerier
E-post är i dag ett arbetsverktyg som används i organisationer världen över – men det utgör också en attackvektor för cyberkriminella. Vissa skadliga e-postmeddelanden är enkla att identifiera på grund av dålig stavning eller okända avsändaradresser. I dag använder cyberkriminella generativ AI för att skapa trovärdiga, perfekt utformade och trovärdiga meddelanden som skickas till tusentals mottagare via e-post, det är också vanligt att dessa e-postmeddelanden förfalskas för att se ut som om de kommer från ett välkänt och pålitligt företag, eller en bekant person. Skadliga program kan även hacka e-postkonton och använda dessa för att skicka skräppost till hela kontaktlistan. Enligt Deloitte inleds 91 procent av alla cyberangrepp via e-posten, där skadliga länkar och bifogade filer använts för att öppna upp bakdörrar åt cyberkriminella.

Microsoft Office-filer
Microsoft Office, som är en välkänd svit av produktivitetsverktyg, innehåller ett kraftfullt skriptspråk för programmering, som gör det möjligt för användare att skapa avancerade funktioner. Detta skriptspråk kan dock missbrukas av brottslingar för att utveckla skadliga skript som installerar skadlig kod eller utför andra skadliga aktiviteter. Man får oftast en varning när man öppnar dessa.

Flyttbara lagringsenheter
En annan metod för spridning av skadlig kod är genom flyttbara lagringsenheter som USB-minnen och externa hårddiskar. När dessa infekterade enheter ansluts till din dator, kan den skadliga programvaran installeras automatiskt.

Installation av applikation
Ibland kan skadlig programvara smyga sig in i ditt system tillsammans med andra program som du laddar ner, särskilt från webbplatser som inte är från de officiella leverantörerna av applikationerna eller via filer delade i privata s.k. P2P-nätverk (peer-to-peer).

Webbplatser och webbläsare
Besök på vissa webbplatser kan leda till cyberangrepp, antingen för att webbplatsen i sig är skadlig eller för att den legitima sidan har blivit hackad. Dessa attacker utnyttjar sårbarheter i din webbläsare. Därför är det av största vikt att alltid uppdatera all programvara till senaste version, särskilt webbläsaren och ta bort oanvända webbläsartillägg.

Att förstå dessa metoder är ett viktigt steg i att skydda din dator och dina personliga data mot cyberhot. Regelbundna uppdateringar, försiktighet med ned-laddningar och e-postmeddelanden, samt säker hantering av flyttbara enheter och applikationer är grundläggande för ett effektivt skydd.

● Hur går ett cyberangrepp till?

De olika faserna

I syfte att belysa hur ett av de vanligaste intrången kan gå till och hur det utförs, kommer vi här att gå igenom de olika faserna av en vanlig attack och hur en hacker kan infiltrera din dator och IT-miljö.

För att kunna ge en inblick i hur en attack går till så kommer vi nedan att förklara hur en av de vanligaste cyberangreppen går till och hur hackare tar sig in i din dator och IT-miljö.

Fas 1: Nätfiskeattacken

Ett vanligt första steg för en hacker är att utföra en nätfiskeattack. Detta innebär ofta att skicka e-postmeddelanden som ser ”äkta” ut, komplett med lockande erbjudanden eller uppmaningar som väcker mottagarens nyfikenhet. När mottagaren klickar på en länk eller bilaga i meddelandet, aktiveras ett litet program som utan mottagarens vetskap startar flera processer i datorn och skapar en bakdörr användarens dator. Inom några sekunder efter klicket etableras en permanent åtkomst för hackaren.

Fas 2: Utforska den interna IT-miljön

När hackaren väl har tillgång till datorn och är inne i systemet, använder denne användarens behörigheter för att söka efter andra datorer i nätverket. Det kan innebära att med hjälp av olika digitala verktyg leta efter delade filer, applikationsdatorer, databas- och webbservrar, och ibland även skrivarens webbgränssnitt, vilket kan ge värdefull information för ytterligare intrång.

Fas 3: Utnyttjande av skrivaren

Skrivare är ofta sårbara punkter som förbises. Hackaren kan utnyttja brister i skrivarens säkerhet, såsom standardlösenord eller inget lösenord alls, för att få åtkomst till högre behörigheter. Denne kan bläddra i skrivarens webbapplikation och komma åt konfigurationsinställningar.

Genom att manipulera inställningarna i skrivaren kan hackaren interagera med andra system i nätverket och med hjälp av digitala verktyg fånga upp e-postadresser, lösenord och användarkonton samt annan information om nätverket som kan vara värdefullt för fortsatta intrång.

Standardinställningen för många skrivare är att tillåta åtkomst till webbapplikationen utan lösenord och finns det ett lösenord glömmer många användare att ändra standardlösenordet som lätt kan hittas i användarmanualer på nätet. Om en hacker får tillgång till en skrivare som har funktionen att skanna dokument och skicka dem som e-postmeddelanden, kan detta utnyttjas för skadliga ändamål.

För att kunna skicka e-postmeddelanden, är kanske skrivaren konfigurerad med ett användarkonto som har högre behörighet än en genomsnittlig användare. Hackare som har digitala verktyg för att få reda på lösenordet till detta konto kan sedan missbruka det för att utföra ytterligare intrång i nätverket eller för att samla in konfidentiell information."

Fas 4: Utvidga Åtkomsten

Med åtkomst till högre behörigheter börjar hackaren utforska IT-miljön mer grundligt. Detta kan innebära att söka igenom filer och känslig information, och hitta administratörskonton som kan användas för att få fullständig kontroll över IT-miljön.
Systematiskt och metodiskt letar hackern igenom all information som han kan komma åt och förr eller senare hittar han uppgifter och inte sällan någonstans gömt i några gamla säkerhetskopior eller gamla delningar ett administratörskonto med tillhörande lösenord

Bristen på överblick på nuvarande IT-miljö och vad tidigare IT-administratörer skapade och aldrig rensade ut gör att man blir sårbar för cyberangrepp. Med hjälp av det stulna lösenordet för administratören får hackaren nu full tillgång till hela IT-miljön, filer, konton, ekonomiska uppgifter och mycket, mycket mer...

Fas 5: Fullständigt Övertagande

I det slutliga steget har hackaren full kontroll över IT-miljön och kan göra vad han eller hon vill, Denna åtkomst kan användas för att kryptera information i en så kallad ransomware-attack, vilket tvingar företaget att betala en lösensumma för att återfå tillgång till sina data.

Hackaren kan också använda IT-resurser från IT-miljön för att sprida eller dela olaglig information på internet samt sprida skadlig kod.

Genom att ha full tillgång till hela IT-miljön och datorn som kontrollerar säkerheten kan hackaren göra i stort sett vad han eller hon vill t.ex. använda ett verktyg för att ladda ner alla användar- och kontouppgifter, alla krypterade lösenord knäcks av ett verktyg som gör miljarder gissningar på några sekunder.

Nu har hackaren full åtkomst och kan logga in med administrativ åtkomst till hela organisationen och kryptera hela eller delar av IT-miljön.

Detta visar hur sofistikerade och skadliga cyberangrepp kan vara och understryker vikten av proaktiva säkerhetsåtgärder för att skydda din IT-miljö.

● Hur skyddar jag mig?

Vad kan jag göra för att förebygga?

Att skydda din IT-miljö från cyberangrepp är en av de mest kritiska utmaningarna som organisationer står inför i dagens digitala tidsålder.

Med cyberhot som ständigt ökar i antal blir det alltmer viktigt att implementera robusta säkerhetsåtgärder för att skydda känslig information. En effektiv strategi inkluderar användningen av avancerad teknik, såsom brandväggar och antivirusprogram, vilka spelar en nyckelroll i att identifiera och avvärja potentiella hot.

Kontinuerlig övervakning av nätverket är avgörande för att snabbt upptäcka och agera på misstänkta aktiviteter. Det är också viktigt att inte underskatta värdet av att utbilda användarna. Genom att informera användarna om de senaste cyberhoten och hur man undviker dem kan många säkerhetsincidenter förhindras redan från början. En kombination av dessa metoder ger en kraftfull grund för att effektivt skydda känslig information och minimera risken för dataintrång och andra säkerhetsrelaterade incidenter.

Nedan är några av de olika system och lösningar samt åtgärder som finns för att säkerställa en organisations cybersäkerhet. Givetvis är storleken på verksamhet relevant för vilken typ av system eller lösning man anser sig ha råd med, men att börja se sig om och reflektera över sitt skydd mot cyberhot är relevant för alla.

"Om du lägger en nyckel under mattan för polisen, kan en inbrottstjuv också hitta den. Brottslingar använder alla tekniska verktyg som står till deras förfogande för att hacka sig in på människors konton. Om de vet att det finns en nyckel gömd någonstans kommer de inte att sluta förrän de hittar den."

- Tim Cook, VD för Apple.

System och lösningar

Microsoft 365

Microsoft 365 erbjuder ett omfattande säkerhetsskydd för att förebygga, upptäcka och hantera cyberhot. Detta skydd inkluderar avancerade anti-phishing-funktioner i Microsoft Defender som varnar för potentiella e-postbedrägerier och ovanliga tecken i avsändaradresser.

Microsoft Defender för Office 365 agerar som en enhetlig säkerhetsplattform som automatiskt detekterar skadligt och misstänkt innehåll över flera applikationer, inklusive e-post och Microsoft Teams. Onedrive for Business erbjuder skydd mot ransomware-attacker genom att tillåta återställning av tidigare versioner av filer. Dessa säkerhetsfunktioner är avgörande för att skydda organisationer mot en mångfald av cyberhot.

Nätverkssegmentering
Nätverkssegmentering är en effektiv strategi för att förbättra cybersäkerheten inom en organisation. Denna metod innebär att man delar upp ett nätverk i mindre delar eller segment. Genom att göra det kan man effektivt begränsa skadan vid en cybersäkerhetsattack, eftersom en angripare som lyckas tränga in i en del av nätverket får svårt att sprida sig till andra delar. Varje segment i ett nätverk kan ha egna säkerhetsregler och åtkomstkontroller. Detta gör det möjligt att skräddarsy säkerhetsnivån för varje del av nätverket beroende på dess känslighet och behov.

Oavsett hur hackare tar sig in i din dator är nätverkssegmentering ett enkelt men mycket effektivt sätt att begränsa hur mycket av ditt nätverk som en hackare kan komma åt om de tar sig in i din miljö

Installera EDR- och XDR-teknik
EDR- (Endpoint Detection and Response) och XDR-teknik (Extended Detection and Response) system som övervakar mycket mer än traditionella antivirusskydd och erbjuder sofistikerade funktioner för att skydda mot cyberhot.

EDR-tekniken fokuserar på att övervaka och skydda enskilda enheter som datorer, servrar och mobila enheter. Systemet övervakar kontinuerligt varje enhet i realtid, samlar in och analyserar data för att identifiera och reagera på ett misstänkt beteende och skadlig aktivitet. Det går snabbt att snabbt hitta och hantera misstänkta aktiviteter samt stoppa säkerhetsincidenter.

XDR-tekniken omfattar en större syn på cybersäkerhet genom att integrera insamling, överföring och mätning från datorer, mobiler, nätverk och molnmiljöer. XDR:s förmåga att samla in, hitta samband och analysera data från olika säkerhetslager möjliggör en snabbare upptäckt och respons på avancerade cyberhot. Systemet erbjuder centraliserad synlighet av säkerhetsläget och automatisering av olika förebyggande säkerhetsåtgärder.

Varje organisation bör avväga att använda EDR och XDR. Båda teknikerna är nödvändiga för att utveckla en effektiv cybersäkerhetsstrategi. Båda använder anpassad detektering av cyberhot och AI-teknologi, för att automatiskt känna igen och svara på hot innan de kan skada organisationen.

“

91%

av alla cyberangrepp inleds via e-posten, där skadliga länkar och bifogade filer använts för att öppna upp bakdörrar åt cyberkriminella.

Källa: Deloitte

Använd verktyg för nätverksdetektering och respons

Network Detection and Response (NDR) är ett mycket effektivt system inom området cybersäkerhet, systemet fungerar genom att övervaka nätverkstrafik för att identifiera och reagera på cybersäkerhetshot.

NDR-lösningar använder avancerade analytiska metoder, som artificiell intelligens (AI) och maskininlärning (ML), för att bygga modeller av normalt nätverksbeteende. Genom kontinuerlig analys av nätverkstrafiken kan dessa system upptäcka avvikande eller skadlig trafik som andra säkerhetsverktyg kan missa. Systemet identifierar en rad olika hot, inklusive okänd skadlig programvara, riktade attacker, insiderattacker och till och med riskabelt beteende från användare.

Använd principen om minsta möjliga privilegium.

Att implementera principen om minsta möjliga privilegium är en grundläggande del av en effektiv cybersäkerhetsstrategi. Denna princip innebär att varje användare, process eller program endast får tillgång till de resurser och privilegier som är absolut nödvändiga för att utföra sina tilldelade uppgifter eller funktioner. Genom att begränsa tillgången till endast det nödvändiga minskar risken för oavsiktliga eller avsiktliga dataintrång och cyberangrepp.

För att effektivt implementera detta bör organisationer genomföra en noggrann analys av användarroller och deras åtkomstbehov för att fastställa lämplig nivå av åtkomst för varje användare eller roll. Principen om minsta möjliga privilegium är en hörnsten i en Zero Trust-säkerhetsmodell, där varje åtkomstbegäran verifieras och valideras, oavsett varifrån den kommer.

AVOKI

Stärk och begränsa åtkomst till kritisk systemkonfiguration.

Att stärka och begränsa åtkomsten till kritisk systemkonfiguration är ett viktigt steg för att förbättra cybersäkerheten. Detta innebär att vidta flera åtgärder för att minska risken för obehörig åtkomst och skydda känslig information.

1. Kräv stark autentisering

Använd starka autentiseringsmetoder, som multifaktorautentisering (MFA), för att skydda webbgränssnitt och andra kritiska system. Detta är särskilt viktigt för tjänster som är tillgängliga externt, som VPN-tjänster.

2. Stänga av onödiga tjänster och segmentera nätverket

Det är viktigt att inaktivera tjänster som inte är nödvändiga och segmentera nätverket för att begränsa åtkomst till kritiska system. Genom att dela upp nätverket i mindre delar, kan du skapa unika säkerhetspolicys och kontroller för varje segment, vilket effektivt hindrar angripare från att röra sig fritt inom nätverket.

3. Rutinmässiga uppdateringar av programvara

Kontinuerliga uppdateringar och förbättringar av programvara är nödvändigt för att skydda mot kända sårbarheter. Regelbunden installation av säkerhetsuppdateringar hjälper till att stänga säkerhetshål som angripare kan utnyttja.

4. Begränsa fysisk åtkomst till nätverksportar

Det är viktigt att begränsa fysisk åtkomst till nätverksportar för att förhindra obehörig åtkomst och potentiella intrång.

5. Använda fil- och enhetskryptering

Kryptering av data, både i vila och under överföring, skyddar känslig information från att bli läst av obehöriga.

6. Installera och använda säkerhetsprogramvara

Det är viktigt att ha en uppdaterad säkerhetsprogramvara, som antivirus och brandväggar, för att skydda mot olika typer av cyberangrepp.

7. Loggning och övervakning

Implementera loggning och övervakningsverktyg för att kunna spåra och analysera misstänkta aktiviteter i systemet.
Genom att implementera några av dessa åtgärder kan organisationer skapa en mer säker och motståndskraftig IT-miljö som är bättre rustad för att stå emot och reagera på cyberhot.

Använd multifaktorautentisering (MFA)

Användningen av multifaktorautentisering (MFA) är en viktig strategi för att stärka cybersäkerheten.

MFA tillämpar en flerskiktsmetod för att säkra data och applikationer genom att kräva att användaren presenterar en kombination av två eller flera autentiseringsfaktorer för att verifiera sin identitet vid inloggning. Detta ökar säkerheten betydligt, eftersom även om en autentiseringsfaktor, såsom ett lösenord, blir känt för en hackare, så kommer en obehörig användare inte att kunna uppfylla det andra autentiseringskravet och därmed inte få tillgång till det fysiska utrymmet, enheten, nätverket eller IT-miljön.

MFA är särskilt effektivt för att skydda mot olika typer av cyberangrepp, inklusive nätfiske, social manipulation och gissningsattacker på lösenord. Det skyddar också mot inloggningar från angripare som utnyttjar svag eller stulen information.

De tre vanliga autentiseringsfaktorerna som används i MFA är något du känner till (t.ex. ett lösenord eller en PIN-kod), något du har (t.ex. en smartphone eller en säkerhetstoken) och något du är (t.ex. biometriska data som fingeravtryck eller ansiktsigenkänning).

Genom att kräva bevis från två eller flera av dessa kategorier skapas en starkare säkerhetsbarriär.

Det är viktigt att tillämpa MFA i din organisation, inte bara för externa servrar utan även för intern administratörsåtkomst. Genom att begränsa åtkomsten till kritiska system med MFA kan du effektivt minska risken för att hackare kan få tillgång till känslig information eller kritiska system.

Genomför penetrationstester

Penetrationstester, utförda av etiska hackare, är en mycket effektivmetod för att identifiera och åtgärda svagheter i ett företags IT-infrastruktur.

Denna process innebär ett simulerat cyberangrepp för att hitta sårbarheter i nätverk och system. Genom att proaktivt identifiera svagheter som kan utnyttjas av hackare, kan ett företag minska risken för framgångsrika dataintrång eller incidenter.

Penetrationstester ger en objektiv bedömning av systemets säkerhetskontroller och upptäcker ofta allvarliga sårbarheter som kan ha förbisetts av automatiska skanningar. Penetrationstester kan kategoriseras i olika tillvägagångssätt, som ger olika insikter beroende på den kunskap som de etiske hackaren har om systemet.

Testerna är inte enbart en teknisk kontroll utan en process som behöver utvecklas och ständigt förbättras över tid

Penetrationstester är nödvändiga för en mogen cybersäkerhetsstrategi och bör inte försummas av företag som vill skydda sin kritiska infrastruktur mot cyberhot.

Microsoft Secure Score

Microsoft Secure Score är ett verktyg för att mäta en verksamhets säkerhetsstatus, resultatet jämför verksamhetens säkerhetsnivå med branschstandarder och Microsofts säkerhetsrekommendationer. Ett högre poäng indikerar bättre säkerhet och poängen hjälper till att mäta framsteg över tiden. Verktyget ger rekommendationer för att förbättra verksamhetens säkerhet, med fokus på att identifiera och åtgärda svagheter i områden som kan förbättras. Verktyget hjälper till att bedöma säkerheten över olika områden som identitet, enheter, information, applikationer och infrastruktur.

> Upp till **70%** minskas riskerna för cyberangrepp genom att utbilda sina användare.
>
> Källa: Aberdeen Group

Genom att jämföra organisationens status över tid och med andra organisationer kan man skapa en plan för att förbättra säkerheten.

Microsoft Secure Score poängen kan vara underlag till rapportering av nuvarande säkerhetsläge samt förbättringar till verksamhetsledning och ligga till grund för förändringar i säkerhetsstrategin. Verktyget är integrerat med andra Microsoft-produkter och kan även ta i beaktning när en tredjepartslösning har använts för att hantera rekommenderade åtgärder. Detta gör det möjligt för att tydliggöra framsteg som görs för att bättre skydda en verksamhets IT-miljö.

Utbildning av användare

Trots att hård- och mjukvaruskydd är viktiga aspekter av cybersäkerhet, kan de inte ensamma fånga upp alla nätfiskeattacker.

Enligt en studie från Aberdeen Group kan utbildning i säkerhetsmedvetenhet minska riskerna med 45–70 %, vilket framhäver vikten av regelbunden och effektiv utbildning för att öka medvetenheten om cybersäkerhet bland användare.

En annan studie från Proofpoint visade att företag som implementerade träning i säkerhetsmedvetenhet såg en minskning med upp till 40 % i antalet skadliga länkar som klickades på av användare.

Detta understryker vikten av att ständigt påminna användare om riskerna samt investera i månatlig utbildning eller information om cybersäkerhet för anställda.

Brandvägg

En brandvägg är en avgörande komponent i en organisations nätverkssäkerhet och fungerar som en barriär för att skydda nätverk mot obehörig åtkomst och cyberhot.

Den kan vara antingen en fysisk enhet (hårdvarubrandvägg) eller en programvara (mjukvarubrandvägg) och är designad för att övervaka och kontrollera inkommande och utgående nätverkstrafik baserat på en uppsättning fördefinierade säkerhetsregler.

Brandväggar placeras ofta mellan Internet och ett privat nätverk, vanligtvis i anslutning till eller inbyggda i en router. Dessa övervakar trafiken mellan nätverken och tillämpar säkerhetsregler för att förhindra oönskad eller skadlig trafik från att nå de interna systemen. Det finns mjukvarubrandväggar som installeras direkt på datorer eller enheter för att ge skydd på individuell nivå.

En brandväggs huvuduppgift är att filtrera nätverkstrafiken och blockera obehöriga försök att få tillgång till ett system eller nätverk. Detta inkluderar att hindra vissa typer av nätfiskeattacker och andra cyberhot.

Men brandväggar kan ha begränsningar, särskilt när det gäller mer sofistikerade nätfiskeförsök som riktar sig direkt mot användare för att få dem att avslöja känslig information.

Regelbunden översyn och uppdatering av brandväggsregler och konfigurationer är nyckeln till att upprätthålla en effektiv nätverkssäkerhet.

Backup – Säkerhetskopiering

Att implementera en strategi för säkerhetskopiering som omfattar flera generationer av säkerhetskopior är en kritisk komponent i en robust strategi för cybersäkerhet.

Cyberhot som ransomware (utpressning) och virus utgör allvarliga risker mot dataintegriteten och där fungerar säkerhetskopiorna som en avgörande säkerhetsåtgärd för att skydda organisationens värdefulla information.

När ett cyberangrepp inträffar, kan effekterna bli katastrofala, antingen låses eller förstörs kritisk information. Genom att ha en säkerhetskopia, dvs. en backup, kan organisationen effektivt återställa sin digitala information från en tidpunkt före attacken. Detta är särskilt värdefullt vid tillfällen där den senaste säkerhetskopian också är utsatt.

Att ha en strategi för flera generationer av säkerhetskopior är inte bara en försäkring mot förlust av data på grund av cyberangrepp, utan även en avgörande komponent i att upprätthålla affärskontinuitet och operativ stabilitet.

Det är en mycket viktig åtgärd som säkerställer att organisationens digitala tillgångar förblir skyddade och tillgängliga, även i en värld av alltmer sofistikerade cyberhot.

> Effekterna av ett cyberangrepp kan få stora konsekvenser för samhällsviktiga funktioner och kritiska IT-system, och de direkta och indirekta kostnaderna för cyberangrepp beräknas till miljardbelopp.

Källa: SÄPO - Säkerhetspolisen

● Vårt unika erbjudande

Hur vår lösning skyddar mot cyberhot

Som ett svar på den komplexitet som råder gällande cybersäkerhet har vi tagit fram två tjänster som tillsammans nyttjar Microsofts XDR lösning (Extended Detection and Response).

Microsoft XDR är ett säkerhetssystem som ger en omfattande och integrerad bild av säkerhetshot, över hela organisationens IT-miljö. Detta inkluderar nätverk, enheter, applikationer och molntjänster.

Tillsammans med Microsoft XDR har vi tagit övervakningen av cyberangrepp ett steg längre. Med hjälp av Artificiell Intelligens och intelligenta rapport- och analysverktyg övervakas din IT-miljö.

Microsoft XDR erbjuder en mängd funktioner, men det kan upplevas som ganska svårnavigerat för gemene man. Det är många inställningar som kan göras och ibland kanske man inte är säker på vad allt gör eller är till för.

Vår tjänst erbjuder en effektiv lösning på detta och vi tagit fram två tjänster som vi erbjuder våra kunder. Vi sköter inställningarna i er Microsoftmiljö utifrån ert unika behov och användarmönster.

AVOKI

● Vårt unika erbjudande

X-One Cloud Security

Med denna unika lösning garanterar vi inte bara skräddarsydd säkerhet baserad på ditt företags specifika behov, utan också en automatisk övervakning som håller dina användare och data skyddad.

Säkerhet med hjälp av Artificiell-Intelligens: Apex Insight

Vår egenutvecklade övervakningsagent säkrar ditt företag och användare med hjälp av Artificiell Intelligens. Med avancerade algoritmer identifierar Apex Insight riskfyllda-, hotfulla beteenden och blockerar användar-konton. När en uppsatt risk- eller hottröskel passerats larmar X-ONE Cloud Security en säkerhetsspeciallist, och ni som kund mottar efter analys en forensisk analysrapport med vad som hänt.

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.

Detaljerade kvartalsinsikter, skräddarsydda för IT och beslutsfattare

Vi tillhandahåller kontinuerliga analyser, uppdateringar och justeringar i ljuset av nya hot och riktlinjer. Detta för att du som kund skall känna dig trygg i att skyddet fungerar samt ha underlag till beslut om något behöver förändras på grund av en ökad hotbild eller en uppdatering av IT-Policy för åtkomst till företagets IT-miljö.

X-ONE 365 Cloud Security kombinerar Microsofts Secure Score med Xites erfarenhet och expertis för en robust 365-miljö. Vi tillhandahåller kontinuerliga analyser, uppdateringar och justeringar i ljuset av nya hot och riktlinjer.

Exempel på inställningar som inkluderas:
Safe attachment policy: granskning av bifogade filer i mail och Teams, **Safe links policy:** skydd mot skadliga länkar för att minska risken för nätfiske, **Antimalware policy:** karantän för misstänkta filer och kod, **Antiphishing policy:** skydd mot identitetsstöld och nätfiske, **Mobile policy:** säkerhet för mobila enheter innan de får åtkomst till 365-miljön.

X-One Endpoint Security / Premium

X-ONE 365 Endpoint Security (EDR), en avancerad säkerhetstjänst som bygger på Microsoft XDR och erbjuder verksamheter en ny nivå av proaktivt skydd. Genom omfattande övervakning och respons, effektiv hantering av digitala enheter som datorer, mobiltelefoner och surfplattor kan du känna dig trygg.

Med detaljerade säkerhetsrapporter och integration med Microsoft Defender for Endpoint, erbjuder denna tjänst en omfattande skyddsmekanism för era IT-system. X-ONE 365 Endpoint Security erbjuder en kontinuerligt uppdaterad, proaktiv säkerhetslösning.

Proaktiv skydd

Säkra dina enheter med ett proaktivt skydd

Övervakning

Kontinuerlig övervakning av skadliga aktiviteter på enheter

Insikter

Detaljerade kvartals-insikter, skräddar-sydda för IT och beslutsfattare

Sofistikerad Övervakning

Genom att övervaka Microsoft Defender, identifierar X-ONE 365 Endpoint Security datorer med riskfyllda beteenden och potentiella virus samt säkerställande av en proaktiv skyddsmetod.

Automatiska larm

När tjänsten upptäcker en risk eller hot, larmas säkerhetstekniker som kan vidta korrekta åtgärder. När tjänsten upptäcker en risk, larmar den ansvariga tekniker och isolerar automatiskt den utsatta enheten för att minska risken för spridning.

Med tillägget Endpoint Security Premium adderas ett antal automatiska åtgärder för att minska spridning, bland annat isolering och avaktivering av enheter samt SMS-larm till ansvariga personer.

Defender Endpoint Hardening

Vid driftsättning av X-ONE 365 Endpoint Security görs en analys med utgångspunkt ifrån Microsofts Exposure Score samt Xites egen expertis. Utifrån detta sätts de regler som behövs för att få en säker och användbar klient/server miljö. Analys och justering av inställningar är ett löpande jobb som ingår i X-ONE 365 Endpoint Security. När nya hot och riktlinjer kommer så uppdaterar vi även er miljö utifrån dessa förutsättningar.

Forensisk Analys

För varje bekräftat hot, genomförs en grundlig forensisk analys. En detaljerad rapport skickas till kunden, innehållande viktig information som datornamn, tidpunkt för riskidentifiering, typ av risk och nivå, samt datorstatus.

Kvartalsrapporter

Varje kvartal mottar du en rapport med utförlig information om säkerheten i er miljö. Denna rapport innefattar företagets exponeringsbetyg, eventuella svagheter i operativsystem och applikationer, samt detaljerad klient/serverinformation.

● Avslutningsvis

Digitaliseringens tidsålder

Avslutningsvis är det viktigt att poängtera att man som företag bör vara medveten om vikten av att skydda sin IT-miljö från cyberangrepp.

Det är avgörande att implementera robusta säkerhetsåtgärder. Se över ert skydd idag och överväg att börja använda avancerad teknik som EDR- och XDR-teknik om ni inte redan har det i er IT-miljö.

Glöm inte bort att regelbunden utbildning i säkerhetsmedvetenhet och penetrationstester är viktiga för att minimera risker och upptäcka svagheter innan hackern gör det.

Mentaliteten att det drabbar andra och inte mig måste ifrågasättas och det är inte en fråga OM jag drabbas utan NÄR. Se till att du är skyddad innan det är för sent.