INNOFACTOR

Den beste sikkerheten i Microsoft-miljøer

Forebyggende digital sikkerhet

- Kunnskapen
- Teknologien
- Prosessene

En guide til smarte sikkerhetsvalg fra Innofactor

Alle arbeidsplasser er fritt vilt

Nasjonalt digitalt risikobilde 2021, publisert av Nasjonal sikkerhetsmyndighet, viser at antallet alvorlige hendelser registrert i 2020 var tre ganger høyere enn året før. Det er også derfor cybersikkerhet bør være forankret i ledergrupper og styrer i alle bedrifter. 2021 lærte oss at ingen er trygge. Hackerne jager bredt på tvers av kommuner, industrien, matprodusenter, mediekonsern og aktører innen reiseliv og turisme.

Alle arbeidsplasser er fritt vilt og floskelen om at det ikke er et spørsmål om «om», men «når» er årsaken til at digital kriminalitet er høyest på listen over trusler som bedriften flagger i sine beredskapsplaner. Bedrifter er eksponert for angripere med økonomiske motiver der krypteringsvirus og «digital utpressing» er særlig utbredt, og i offentlig sektor foregår komplekse angrep for å svekke vår stats- og samfunnssikkerhet. Angrepene er i dag så målrettet at selv de minste bedrifter utsettes for sofistikerte svindelforsøk.

I dette whitepaperet får du gode råd om hva du bør tenke på for å sikre ditt Microsoft-miljø på en best mulig måte. Du kan også lese om hvordan den skybaserte SIEM-løsningen Microsoft Sentinel gjør virksomheten bedre rustet mot angrep, og hjelper deg med å redusere nedetiden hvis angrepet skulle lykkes.

God lesning!

INNOFACTOR

Det har aldri vært mer populært å være sikkerhetsekspert

Selv små og raske grep kan heve sikkerhetsnivået betraktelig. Men det krever at man har den nødvendige sikkerhetskompetansen, eller kjøper dette som en tjeneste.

Sikkerhetskompetanse er blitt noe av det vanskeligste å skaffe nok av. Den eneste måten sikkerhetsproblemene kan adresseres er ved å skaffe seg tilgang på god nok kompetanse. Heldigvis er det mulig å kjøpe den sikkerhetskompetansen man mangler selv fra eksterne aktører, noe også Nasjonal Sikkerhetsmyndighet (NSM) anbefaler at man gjør ved behov.

Fordi de fleste vellykkede angrep forårsakes av menneskelige feil må IT-avdelingen legge til grunn et regime der de har null tillit (zero trust) som førende prinsipp. Hull må hele tiden tettes, angrep og risiko proaktivt avdekkes og fjernes, skadelige e-poster må holdes ute, ondsinnede lenker sperres, og de ansatte bør få anledning til å jobbe trygt uten frykt for at de risikerer bedriftens fremtid ved å gjøre utilsiktede feil. Sikkerhetsekspertens jobb er å sikre at kollegene kan være trygge, og dermed må løsningene være «idiot-sikre».

Sikkerhetsbalansen

Er sikkerheten god nok vil angripere foretrekke å banke på naboens port, som er enklere å komme gjennom. Det er en overflod av arbeidsplasser med slett sikring av sine Microsoft-miljø. Derfor vil selv små og raske grep bidra til å heve sikkerhetsnivået betraktelig. I skyen handler det om å skru på sikkerhetsfunksjoner som de fleste allerede har betalt for, men at dette gjøres av kyndig og erfarent personell for at ansatte skal få utført sine arbeidsoppgaver på en måte som oppleves effektiv og fleksibel, uansett tid og sted. Grunnprinsippet er at mennesker, maskiner og megabytes må sikres, men ikke på en måte som hemmer bedriftens konkurransekraft. Dette er særlig viktig i en tid der hjemmekontor og fleksible arbeidsformer er den nye normalen.

Må prioritere det forebyggende

IT-avdelingens rolle i dette arbeidet er å legge til rette for et sikkerhetsregime der den mest avanserte teknologien stopper fiendene ved porten. Beste praksis og bruk av riktig Microsoft-teknologi er tilstrekkelig for å stå imot nær alle former for angrep. Den viktigste delen av denne oppskriften handler om det kritiske arbeidet med å innføre løsninger som oppdager og fjerner trusler lenge før menneskene oppdager at de utgjør et problem, der særlig smarte nye skyfunksjoner hever mulighetene til et nytt nivå.

Direktør i Næringslivets sikkerhetsråd, Odin Johannesen, uttaler på organisasjonens egne nettsider at «dersom jeg skal velge ett område jeg ville prioritert sikkerhetsarbeidet mot i 2022, er det forebyggende digital sikkerhet».

FAKTABOKS

De unge er mest utsatt

En undersøkelse publisert av Mediatilsynet i desember 2021 viser at de yngre er overrepresentert når det gjelder personvernangrep, som å bli lurt fra passord og få publisert bilder av seg selv mot sin egen vilje. Samtidig viser undersøkelsen at eldre nettbrukere er de som finner det vanskeligst å stå imot kommersielt press i form av at de lures til å kjøpe noe, eller fortsetter å betale for tjenester de trodde de hadde avviklet.

FAKTABOKS

Ledere føler seg ikke trygge på lagring i skyen

600 ledere i privat sektor ble høsten 2021 intervjuet av Scentio Research på vegne av CapGemini. Svarene etterlater ingen tvil om at ledere opplever at skyen er kritisk for å skjerpe bedriftens konkurransekraft, til tross for at det er en utbredt usikkerhet knyttet til om løsningene er trygge nok. Derfor svarer en av to ledere at de tror det er tryggest å lagre interne data på lokale servere, i eget hus eller driftet eksternt. Videre svarer seks av ti ledere at de enten mener bedriften har for liten kunnskap om skytjenester, eller hvordan de kan utnyttes best mulig.

Fem veier til god nok sikkerhet

«Det skal smelle andre steder enn hos deg», sier de erfarne sikkerhetskonsulentene.

Trønderen Jens Røttereng og Lasse Wedø fra Bergen er samstemte: Få bedrifter er gode nok på å sikre sine Microsoft 365-miljøer. Herrene har gjennom hele karrieren jobbet med IT-sikkerhet, nå i Innofactor. Begge er blant de fremste i landet på hvordan legge til rette for riktig sikkerhet i Microsoft-miljøer.

Lasse Wedø

Jens Røttereng

– Under pandemien har nær alle bedrifter skrudd på Teams, men altfor få vet hvilke implikasjoner dette egentlig har for sikkerhet, og de har heller ikke skrudd på sikkerhetsfunksjonene de allerede har betalt for, sier Røttereng.

Målet deres er ikke å tjene godt på utrykninger når det smeller hos kundene. Jobben skal gjøres i forkant.

– Vi skal gjøre IT-miljøet så trygt at om en hacker forsøker seg så går han heller videre til noen som det er enklere å bryte seg inn hos. Og akkurat det er ikke vanskelig å finne. Vår jobb er å sikre at det smeller andre steder, og om det mot formodning skulle smelle hos våre kunder skal effekten være minimal og enkel å håndtere, sier Wedø.

Det som er viktig å forstå er at mye av dagens uønskede aktiviteter ikke handler om å få tak i bedriftshemmeligheter, men å finne hull i sikkerheten som kan brukes til å infisere og lamme hele bedriften (løsepengevirus o.l.)

Har sett det meste

Innofactors styrke er at selskapet er Norges fremste konsulenthus på Microsoft-teknologi. Få har flere og mer erfarne konsulenter på programvaregigantens sikkerhetsportefølje, etter tusenvis av oppdrag hos virksomheter av alle størrelser på tvers av Norden i mange år.

– Vi har stor oversiktskompetanse og har sett det meste. Vi er gode til å se helheten, og vet hva kundene skal gjøre for å trygge sine omgivelser, sier Røttereng.

Wedø forklarer at det er ikke mye som skal til for at bedriften skal komme over i en tilværelse der de har oppimot 98 prosent sikkerhetsgrad. Og det vil i de fleste tilfeller være mer enn nok til at angriperne ikke tar seg bryet, når det er så mange enklere fisk å fange.
Sikkerhetsansvarlig må ha kontroll på identitetene og enhetene i bedriften, verktøy for å hindre at data kommer på avveie, og da særlig sensitive personopplysninger, og ikke minst ivareta at programvare og maskinvare alltid er oppdatert, der tjenester er konfigurert riktig slik at ansatte ikke kan klikke på skadelige lenker.

INNOFACTOR

Fem grep som bør tas

Wedø fremhever disse fem grepene som viktige for å heve sikkerhet:

- Tofaktor-autentisering
- Klientbeskyttelse
- Tilgangskontroll
- Databeskyttelse
- Sikre at maskinparken og programvaren er oppdatert

– Dette handler om teknologi og prosesser der sikkerheten adresseres hele tiden. Teknologien har veldig mange allerede betalt for i sine programvarelisenser, og det handler om å vite om hvilke funksjoner som bør skrus på, sier Wedø.

Røttereng peker på at det er viktig å ha kontroll på brukernes påloggingermønster slik at det er mulig å luke ut unormal oppførsel, som å fange opp at kollegaen du så i går trolig ikke kan logge seg på fra Mongolia i dag.

Ikke stol på noen

Sikkerhetsekspertene mener arbeidsmetodikken skal preges av at man ikke stoler på noen; Zero Trust. Det handler om å være før var, der sikkerheten er allerede gjennomtenkt før nye skytjenester skrus på.

– Microsoft har allerede programvaren som er nødvendig for å lykkes med en slik strategi, og ingen leverandører investerer mer i utviklingen av gode og programvaredefinerte sikkerhetsløsninger, sier Wedø.

I en tid der bedrifter raskt har begynt å jobbe med data på nye måter, der filer deles annerledes, må sikkerheten støtte dette. 98 prosents beskyttelse mot digital kriminalitet inneholder oppskriften der bedriften har:

- Mekanismer som stopper uønskede e-poster
- Beskyttelse som hindrer at skadelige e-poster kan åpnes
- Løsninger som skal hindre at farlige lenker kan klikkes på
- Systemer som avdekker unormal adferd og påloggingerfra usannsynlige steder

– Balansen er viktigst. Sikres alt og alle ting, er det heller ikke mulig for de ansatte å få gjort jobben sin. God sikkerhet krever forretningsforståelse, sier Røttereng.

FAKTABOKS

Visste du at..

- 80 % av dagens sikkerhetsbrudd er relatert til identiteter og tilganger?
- 52 % av sikkerhetsbruddene i små virksomheter oppdages ved en ren tilfeldighet? [1]
- 8 av 10 datainnbrudd i sky- og lagringstjenester er knyttet til kompromitterte passord?
- Løsepengevirus er de vanligste – og mest økende – truslene mot små og mellomstore bedrifter i Norge og Europa [1]?
- Dataangrep kan bety enorme kostnader? Eksempelvis hadde dataangrepet som rammet norske Hydro i 2019, en samlet kostnad på 800 millioner kroner [2]

[1] Norsis

[2] Aftenposten

FAKTABOKS

Forbyr dårlige passord

På tampen av 2021 vedtok de britiske myndighetene en lov som heter Product Security and Telecommunications Infrastructure. Et av de viktigste formålene med loven er å skjerpe datasikkerheten med egne lover som skal gi bedre vern mot hacking. Et virkemiddel er å hindre produsenter å utstyre produkter og IoT-utstyr med standardpassord som er enkle å gjette seg frem til. Det innebærer at alle enheter må utstyres med unike passord, og brudd på disse reglene kan medføre bøter på inntil 10 millioner britiske pund.

INNOFACTOR

Trygghet som en tjeneste:

Microsoft Sentinel – et «cloud native» SIEM-verktøy som er raskt og enkelt å rulle ut

Det finnes mange sikkerhetsprodukter det er viktig å ha kontroll på, og det er utfordringer knyttet til å integrere mange av de med hverandre. Skyplattformen Microsoft Sentinel er designet for å gi kontroll — og skalere på tvers av dine IT-miljøer.

En SIEM-løsning (Security information and event management) gjør det mulig å samle og få oversikt over sikkerhetshendelser, både for å kunne avdekke trusler i tide og for å stå bedre rustet den dagen angrepet er et faktum. Men SIEM-løsninger har tradisjonelt vært dyre i drift, kompliserte å sette opp, de har skalert dårlig – og de har gitt altfor mange advarsler.

Skyplattformen Microsoft Sentinel er designet for å gi kontroll – og skalere på tvers av dine IT-miljøer.

INNOFACTOR

Derfor satser Innofactor stort på den relativt nye plattformen Sentinel fra Microsoft. Sentinel bygger på Microsofts sikkerhetserfaring gjennom mange tiår, og er bygget helt fra grunnen av som en «cloud native»-løsning.

Siden Microsoft Sentinel er en skybasert løsning, trenger du ikke å sette opp noen infrastruktur selv for å ta løsningen i bruk.

– Med noen klikk så har man gjort den initielle utrullingen og man er klar for videre konfigurereing. Underliggende infrastruktur skalerer automatisk etter hvert som behovene endrer seg, sier Haakon Baglo, seniorkonsulent i Innofactor.

Haakon Baglo,
seniorkonsulent i Innofactor

INNOFACTOR

Stor angrepsflate og mange veier inn for en angriper

Baglo forteller at mange selskaper dessverre er reaktive når det gjelder hvordan de tenker IT-sikkerhet. Det betyr at de ofte oppdager sikkerhetsbrudd altfor sent – enten det er skadevare, digital utpressing, utro tjenere og innsidetrusler, eller andre trusler.

– Det digitale fotavtrykket til bedriftene har blitt større. Dagens sikkerhetsscenario er mer komplekst, og for angriperne ligger det mye verdi i det å utnytte at selskapene er sårbare og at det er vanskelig å sikre alt godt, sier Baglo.

Det er en stor utfordring for moderne virksomheter at angrepsflaten er mye større enn den var for bare få år siden. Angriperne har rett og slett veldig mange flere veier inn enn de hadde tidligere. Brukere og enheter er spredd på mange ulike lokasjoner, noen befinner seg i bedriftens interne nettverk, andre på hjemmekontorer, ute hos kunder eller andre steder. Samtidig er også applikasjonene og tjenestene spredd. Applikasjoner eller data ligger kanskje på en on-premise server, man har gjerne mange ulike offentlige og private skyløsninger, noe ligger på edge-lokasjoner, og så videre.

– Det er her et godt SIEM-verktøy kommer inn. Det henter informasjon fra logger og ulike kilder og sentraliserer det, slik at du får veldig god oversikt over alt det komplekse som skjer på ett sted. Dermed kan du gå fra å være reaktiv til proaktiv, sier Baglo.

Nils-Ove Gamlem, Sr. Enterprise Security Executive i Microsoft Norge forteller at de fleste angrep starter ett sted før angriperne beveger seg rundt i infrastrukturen til de til slutt finner ut hvordan de skal gjennomføre angrepet og hente ut data. Ofte kan angriperne ha hatt tilgang til systemene i lang tid.

Nils-Ove Gamlem,
Senior Enterprise Security
Executive i Microsoft Norge
(Foto: Microsoft).

Kompleksiteten i moderne IT-systemer stiller nye krav til sikkerhetsløsningene for at sikkerhetstrusler skal kunne avsløres tidlig.

– Det er ikke som «i gamle dager» der du bare kunne «tappe inn i» nettverket ditt for å få oversikt over alt som rører seg av hendelser og avvik. I dag må du plugge deg inn et stort antall steder, forklarer Gamlem.

Mer enn 150 connectorer

Haakon Baglo i Innofactor mener en av de store styrkene til Sentinel sammenlignet med andre SIEM-løsninger, er hvor enkel den er å sette opp og at den kommer med mer enn 150 integrasjoner mot ulike løsninger. Dermed er det enkelt å konfigurere løsningen til å hente generiske logger fra servere, hente logger fra brannmurer fra for eksempel Cisco, Check Point eller Palo Alto, eller samle data fra mange ulike skytjenester.

Data som kommer fra andre Microsoft-løsninger kan prosesseres i Sentinel kostnadsfritt, for eksempel aktivitetslogger fra Azure eller logger fra Office 365 – og så er det mulig å kjøpe lagring av eventer og alarmer for inntil to år. I tillegg er hendelser fra Microsoft 365 Defender nå integrert med Sentinel, slik at du får en mer sømløs brukeropplevelse og måte å respondere på sikkerhetstrusler på. Med ett klikk vil hendelser fra Defender dukke opp automatisk i hendelseskøen i Sentinel og kan bli prioritert og beriket med data fra andre kilder.

– Det betyr at virksomheter veldig raskt kan komme opp på et godt nivå sikkerhetsmessig, sier Baglo.

Tidligere var det bare de aller største virksomhetene som brukte SIEM-verktøy, men med Sentinel er terskelen for å komme i gang senket betraktelig. Dermed er SIEM noe også mindre bedrifter kan ha god nytte av.

– Det fine med Sentinel er at den lever i Azure-tenanten til kunden, og det er kunden som eier dataene og har abonnementet på Azure. Kunden kan delegere tilgang til partnere – det er flere som tilbyr såkalt «managed SOC» hvor du får SOC som en tjeneste. Men det er fortsatt kundens SIEM, og vil du bytte til en annen leverandør senere er det ikke noe problem, sier Nils-Ove Gamlem i Microsoft.

Baglo legger til at det å kjøpe en SOC-tjeneste kan være dyrt og ikke er for alle.

– Men med Sentinel får du et verktøy som sikrer deg godt, og du har mulighet til å få veldig mye av det som ligger i en SOC-tjeneste rimelig, sier Baglo.

Kunstig intelligens og maskinlæring gjør at du slipper å «drukne» i alarmer

Det kan være komplisert og uoversiktlig å samle signaler fra brukere, PC-er, servere, applikasjoner, ulike skytjenester– og se alt i en sammenheng. Antallet alarmer kan fort bli så stort at det kan være vanskelig å skille legitime hendelser fra sikkerhetshendelser som bør undersøkes nærmere.

– Det er viktig å unngå «alarmtrettheten» man får hvis man nærmest drukner i alarmer. Sentinel samler og korrelerer et stort antall hendelser og gir deg en prioritert liste over alarmer. Av tusenvis av alarmer er det kanskje bare en liten håndfull som er kritiske og som man må ta tak i, sier Gamlem.

Takket være bruk av kunstig intelligens, maskinlæring og erfaringen Sentinel får gjennom analyse av flere billioner signaler daglig fra kunder over hele verden, reduseres støyen fra legitime hendelser slik at du får oversikt over det som betyr noe ut fra et sikkerhetsperspektiv. I praksis betyr det at du kan reagere raskere på trusler.

Kunstig intelligens og maskinlæring brukes også til å oppdage unormal oppførsel fra kompromitterte brukere, eller innsidetrusler som for eksempel «utro tjenere».

INNOFACTOR

– Vi bruker maskinlæring som lærer nettverket og brukerne å kjenne. Ett eksempel kan være for eksempel hvis mengden data som lastes ned fra en bruker plutselig en dag går utenfor normalen. Og så kan Sentinel detektere det vi kaller «impossible travel». Hvis samme bruker logger på i Oslo klokken 12 og i Kuala Lumpur kl 12:15, da kan sesjonen til brukeren termineres. Og så kan man tvinge passordbytte og tofaktorautentisering ved neste innlogging.

Aldri 100 % trygg – men du kan være bedre rustet hvis noe skjer

Gamlem mener at SIEM-verktøy blir viktigere og viktigere innenfor IT-sikkerhet, også med tanke på «zero trust» – at man aldri skal stole på noen brukere eller enheter.

– Uansett hvor mye man prøver å sikre seg, så kan du aldri være 100 % sikker – selv om vi selvsagt bør tilstrebe det. Man trenger derfor et verktøy også for å håndtere situasjoner der et angrep faktisk har skjedd.

Hvis uhellet mot formodning skulle være ute, er det viktig å ha kontroll på logger. Det er ikke bare for å stoppe angrepet, men også for å kunne få et klart bilde av alt som har foregått. Hvor stort er omfanget av angrepet? Har data kommet på avveie?

– SIEM kan også være et godt preventivt verktøy. Det kan ikke bare brukes til etterforskning hvis noe går galt, men til å få et godt overblikk over hvordan det står til med sikkerheten i virksomheten. Har vi skrudd på de rette tingene og konfigurert alt riktig? sier Gamlem.

Det å ha god kontroll på alt av loggdata er også viktig for å kunne vite når angriperne først hadde tilgang til systemene, slik at systemene kan gjenopprettes uten datatap og med minst mulig nedetid.

– Med Sentinel får du i praksis trygghet levert som en tjeneste.

For å hjelpe kundene i gang med Sentinel bistår Innofactor med en trestegsmodell som gir gode og nøyaktige beslutningsgrunnlag, der en del av jobben også innebærer å koble programvaren på noen av bedriftens datakilder.

– Det gir et nøyaktig bilde av hvor mye sikkerheten blir, og mange blir også overrasket over at investeringen betaler seg såpass raskt tilbake, sier Baglo.

Fire viktige egenskaper ved Sentinel

Microsoft Sentinel gir deg intelligent sikkerhetsanalyse for hele virksomheten, ved blant annet å:

- **Samle inn** data fra alle kilder; fra logger i skyer, brukere, enheter, applikasjoner og fra selve infrastrukturen. Dette i alt fra multisky-miljø til systemene du har i egne datasenter
- **Oppdage** tidligere avdekkede trusler og minimere falske positiver ved hjelp av analyse og trusselintelligens fra Microsoft
- **Undersøke** trusler med kunstig intelligens og jakt på mistenkelige aktiviteter i stor skala, med å utnytte flere tiår med cybersikkerhet hos Microsoft
- **Svare** raskt på hendelser med innebygd iverksetting og automatisering av vanlige oppgaver

FAKTABOKS

Svekket sikkerhet hjemme

Nærmere tre av ti virksomheter opplevde at IT-sikkerheten deres var svekket i løpet av de første ukene med hjemmekontor under koronakrisen. Derfor er det helt avgjørende for en virksomhet at alle ledere, spesielt innenfor offentlig sektor, er sitt ansvar bevisst og tilbyr sine ansatte grunnleggende opplæring slik at de kan avsløre svindelforsøk og andre typer cybertrusler før det rammer de ansatte eller virksomheten. Undersøkelsen er gjennomført av Næringslivets sikkerhetsråd (NSR) i form av intervjuer i hele 900 virksomheter. Generelt opplevde en av ti spurte at ansatte på hjemmekontor svekket IT-sikkerheten deres. Innenfor offentlig sektor var denne andelen nesten tre ganger så høy (28 %). Deretter følger undervisningssektoren (24 %)

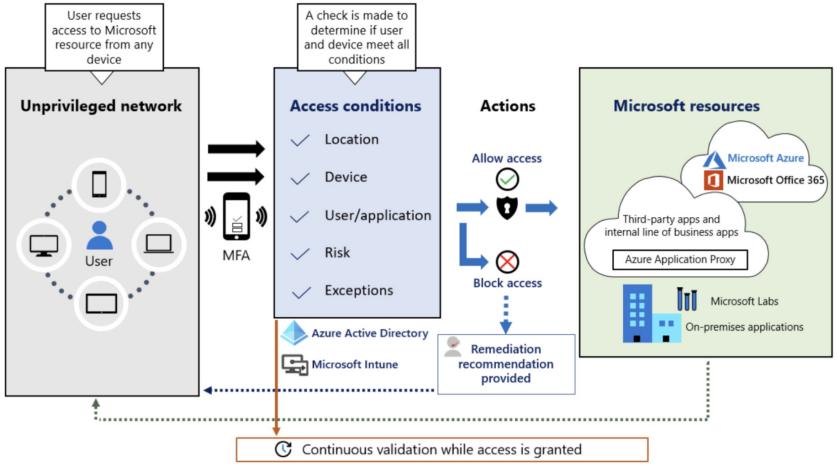
INNOFACTOR

Sikkerhet og kontroll uansett hvor brukerne eller dataene befinner seg

Sikkerheten som er innebygget i Windows, kombinert med moderne skybasert klienthåndtering, gir en helt annen kontroll og funksjonalitet enn hva vi har vært vant til fra tidligere.

I dagens trusselbilde er sikring av bedriftens data viktigere – og vanskeligere – enn noensinne. Det viktigste du kan gjøre for å unngå å bli rammet, er å innføre zero trust, forteller Nicolai Henriksen, Principal Solution Architect i Innofactor.

Zero trust innebærer at man ikke skal stole på noen, verken enheter eller brukere. Hver enhet og bruker får tilgang til kun det som trengs, blant annet gjennom løsninger for tilgangsstyring og administrasjon av identiteter.



Du kommer selvfølgelig heller ikke utenom skikkelig endepunktsikkerhet og administrasjon av PC-er og andre enheter (endepunktsikring).

– Det er ekstremt viktig å ha god administrasjon av sikkerhet og at du beskytter bedriftsdata. Dataene befinner seg ikke lenger bare på en disk på innsiden av bedriftens nettverk. De er tilgjengelig overalt der brukerne befinner seg, i bedriftens nettverk og i ulike skytjenester. Derfor må du sikre enhetene og brukerne, uansett hvor de måtte befinne seg, sier Henriksen.

Han sier at mange glemmer at man trenger sikkerhet i skyen i sin iver etter å ta i bruk stadig nye former for skytjenester. At noe befinner seg i skyen, betyr ikke at det automatisk er sikkert – man må tenke helhetlig sikkerhet.

Mer avanserte angrep gjør at du må tenke nytt rundt sikkerhet

Angrepene er mye mer avanserte nå, og spesielt de siste fem årene har digital utpressing – populært kalt «løsepengeangrep» – vært et stort problem i Norge og resten av verden.

– Det har blitt vanlig med phishing-angrep der du blir lurt til å klikke på en lenke i en epost som ser ut som den kommer fra en kollega, eller på andre måter ser ut til å være viktig. Ofte kan epostene være godt skrevet, og brukeren lures til å installere skadelig kode på maskinen som gjerne kan ligge der i ukesvis eller månedsvis, inntil angriperen har fått kontroll over nok maskiner.

Henriksen forteller at det ofte benyttes sårbarheter i programvare på PC-en, for eksempel i nettleseren.

– Script som kommer via nettleseren er vanlig. Men løsepengevirus har blitt et spesielt stort problem. Penger driver alt, og angriperne vil ha penger for bedriftsdataene.

Solid kompetanse på endepunktsikkerhet

Henriksen har jobbet som IT-konsulent med fokus på administrasjon og sikkerhet i mer enn 22 år. Han var i 2012 den første i Norge som ble MVP (Most Valuable Professional) for produktet Endpoint Manager (SCCM og Intune) – over en periode på 8 år. Dette er en tittel som gis kun til noen få av de fremste Microsoft-ekspertene i verden.

Spesielt endepunktsikkerhet er en stor lidenskap for den erfarne sikkerhetskonsulenten i Innofactor.

– Sikkerhet på klienter har vært en stor interesse helt siden 90-tallet, forteller Henriksen, som også har skrevet bok om Microsofts løsninger for endepunktbeskyttelse – på oppdrag fra Microsoft. Boken er utgitt på det britiske forlaget Packt og er tilgjengelig via Amazon.

Henriksen mener det er viktig å være oppmerksom på kostnadene ved å administrere.

– Noen IT-avdelinger trenger kanskje ikke enda et system å administrere, det de trenger er å avlastes med løsninger som kan forenkle og automatisere. Da trenger du noen som kan se hele bildet og gi råd om hva man trenger, til en overkommelig pris.

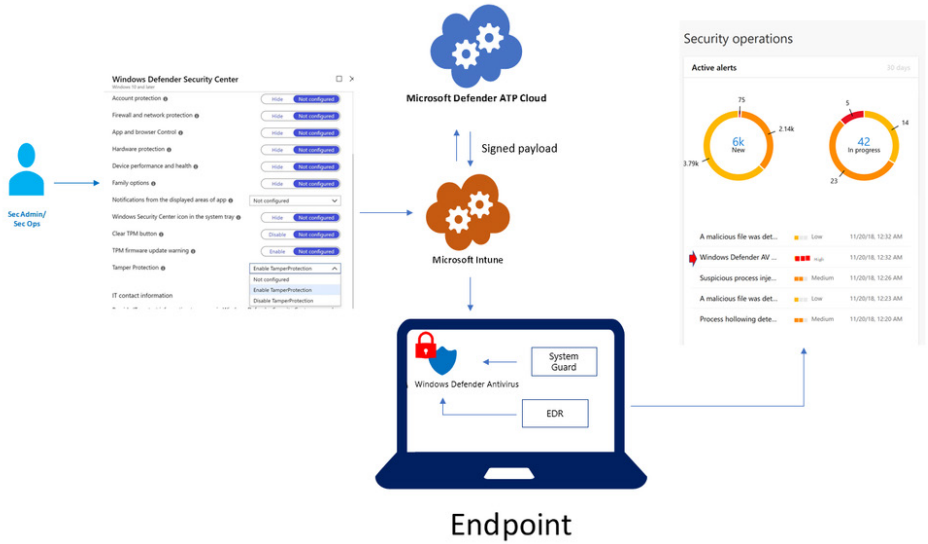
Han mener det er et stort pluss at Innofactor ikke skal selge kun én bestemt løsning, men har kompetanse og erfaring med mange ulike løsninger.

INNOFACTOR

– Det er viktig for kundene våre å jobbe med noen som kan ha et objektivt syn.

Henriksen er likevel klar på at selv om behovene kan være ulike, så vil mange bedrifter med Windows-miljøer være godt tjent med å utnytte mulighetene som ligger i Microsofts egne løsninger enda bedre.

– Vi tar en full gjennomgang med kundene. Det viser seg for eksempel ofte at noen er lisensiert til å ta i bruk funksjoner de ikke har skrudd på.



Moderne klienthåndtering med Microsoft Defender 365 og Intune

Alle Windows-PC-er kommer med sikkerhetsplattformen Microsoft Defender Antivirus innebygget. Dette er en viktig komponent i Microsoft Defender for Endpoint, hvor beskyttelse av PC-ene (endepunktene) kombineres med Microsofts skybaserte løsninger for sikring av endepunktene ved bruk av blant annet maskinlæring og avansert analyse.

Henriksen mener de fleste ikke lenger har behov for tradisjonelle antivirusløsninger som installeres på PC-ene på toppen av Microsoft Defender.

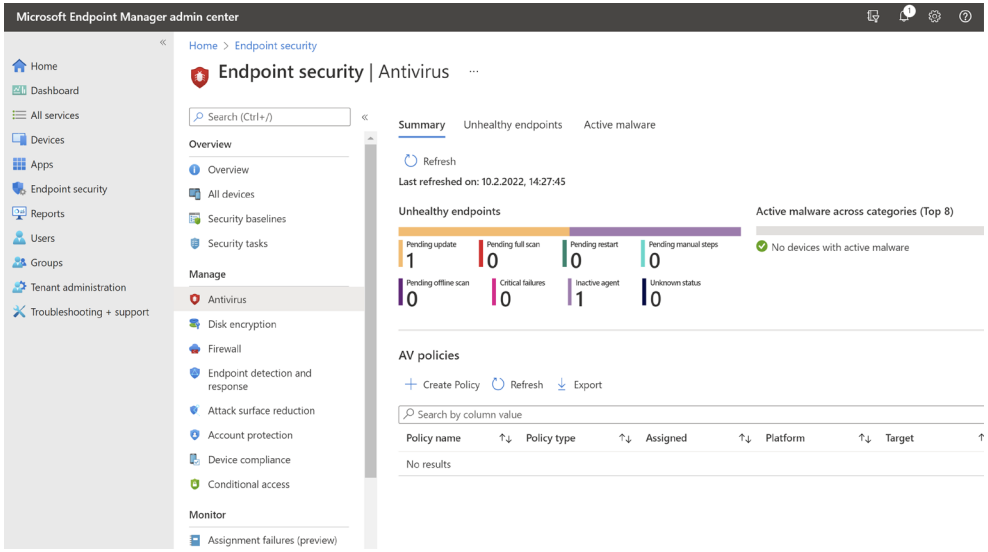
– Defender ligger jo allerede på maskinen. Ettersom alt er innebygget og tett integrert i Windows slipper man mye av den overheaden man har med gammeldagse antivirusløsninger. Du slipper å installere en masse ekstra komponenter og ha en mengde ulike policyer. Dette var noe som tidligere kunne forsinke påloggingstiden til klienten med flere minutter, sier Henriksen.

Alle klientene kan administreres via skyløsningen Microsoft Intune eller Configuration Manager. Defender ligger på hver PC og samler og prosesserer data og sender det til skyen.

– Med moderne klienthåndtering med Intune og Azure og sikkerheten som er i Windows, så får du en ekstremt bra brukeropplevelse. Brukerne har rask pålogging, og bedriften kan administrere klientene fra hvor som helst og sørge for at alt er patchet og sikret. Det gir en helt annen kontroll enn man hadde tidligere.

Gjennom analysefunksjonaliteten i Intune får man en analyse av alle Windows-enhetene i bedriften, blant annet hvor raskt PC-ene starter opp, om de har noen problemer, om det har oppstått programkrasjer, eller om de er klare for å oppgraderes til Windows 11.

– Det gjør at du for eksempel enkelt kan se hvilke maskiner som er modne for utskiftning. Mange bedrifter sliter i dag også med å ha kontroll på patching og oppdateringer, noe du får god oversikt over i Intune.



Sett krav til hvilke enheter som skal få tilgang

PC-er som ikke er oppdatert kan være en sikkerhetsrisiko, men ved å bruke såkalt «conditional access» kan Microsoft Intune kontrollere hvilke klienter og applikasjoner som skal få lov til å ha tilgang til bedriftens data.

– Du kan for eksempel sette opp at hvis brukere skal få tilgang til bedriftsdata, så må de ha en maskin som er sikret med krypteringsverktøyet BitLocker, har antivirus, er patchet, og så videre. Du definerer kriteriene, så får brukeren beskjed hvis PC-en ikke oppfyller kravene – med forslag til hvordan de kan løse det selv, eller ved å ta kontakt med IT.

En nyhet i Defender 365 som enkelte av Innofactors kunder har tatt i bruk,er at bedriften kan spore og regulere tilgang til nettsider basert på innholdskategori. Det behøver ikke nødvendigvis være nettsider med skadelig innhold, men nettsider man likevel ikke ønsker at ansatte skal besøke – for eksempel porno, gambling eller nettsider som leverer eller promoterer ulovlig innhold.

– Det fine er at denne og mange andre funksjoner allerede er innebygget i Defender. Når en maskin er innrullert, kan man enkelt aktivere Defender i skykonsollet i Azure, sier Nicolai Henriksen.

La brukerne hjelpe seg selv

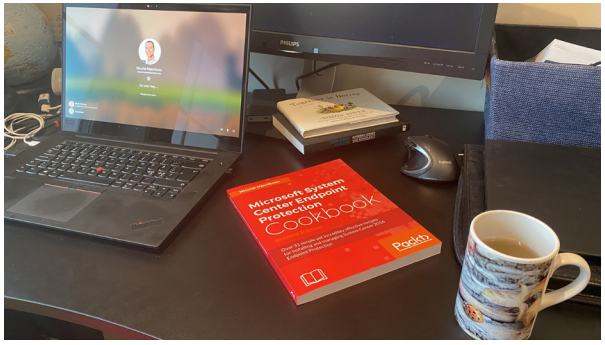
Innofactor jobber mye med å hjelpe kundene med å gjøre brukerne mer selvhjulpne.

Windows Autopilot er en løsning som brukes for å sette opp og forhåndskonfigurere nye PC-er, slik at det blir enklere for IT-avdelingen å håndtere hele livssyklusen til PC-ene. Når en ansatt trenger en ny PC, kan den sendes hjem til vedkommende og brukeren kan selv logge seg på og få PC-en automatisk satt opp med de applikasjonene, innstillingene og sikkerhetspolicyene bedriften har valgt.

– Brukerne blir mer selvhjulpne, sier Nicolai Henriksen i Innofactor.

Når PC-ene er innrullert kan den administreres via Configuration Manager eller den skybaserte løsningen Microsoft Intune. Henriksen forteller at mange kunder fortsatt bruker Configuration Manager, som vil være støttet i lang tid fremover. Men trenden er at stadig flere velger Intune-løsningen, som er integrert med Azure Active Directory (Azure AD).

– Du trenger imidlertid ikke kaste ut Configuration Manager for å begynne å bruke Intune, men kan ta i bruk såkalt «co-management» ved å lage en kobling mellom Configuration Manager og Intune. Fordelen med det er at alt er i synk, og du kan administrere klienter fra begge steder.



Nicolai Henriksen har skrevet bok om Microsofts løsninger for endepunktbeskyttelse – på oppdrag fra Microsoft. Boken er utgitt på det britiske forlaget Packt og er tilgjengelig via Amazon.

INNOFACTOR