Digitalisering stiller nye krav til IT-Sikkerhet

evelon

FORORD

Den digitale transformasjonen stiller stadig nye og strengere krav til virksomheters sikkerhetsløsninger. Likevel behøver det verken å være vanskelig eller komplisert å finne passende og kostnadseffektive løsninger til din virksomhet.

Mørketallsundersøkelsen, som foretas av Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget, kartlegger omfanget av datakriminalitet og sikkerhetshendelser relatert til IT i Norge. Undersøkelsen tar for seg hvor bevisste norske virksomheter er på informasjonssikring, og i hvor stor grad de har nødvendige sikringstiltak etablert.

Har du noen gang tenkt på hvordan din virksomhet er sikret mot dagens trusselbilde, eller hvordan GDPR kommer til å påvirke virksomheten når regelverket trer i kraft 1. juli 2018? Vet for eksempel dine ansatte hvordan de kan se om et vedlegg inneholder skadevare? Har virksomheten ekstra beskyttelse for data som inneholder personsensitive data?

Det handler om å implementere løsninger som bidrar til økt informasjons og personsikkerhet, samt hjelpe ansatte til å forstå hvordan de kan bidra til å redusere sjansen for sikkerhetsbrudd i virksomheten. Start deres digitale sikkerhetsreise nå, og ta kontakt med meg dersom dere har spørsmål eller trenger hjelp.

Andreas Schøyen
Teknologidirektør,
Evelon AS

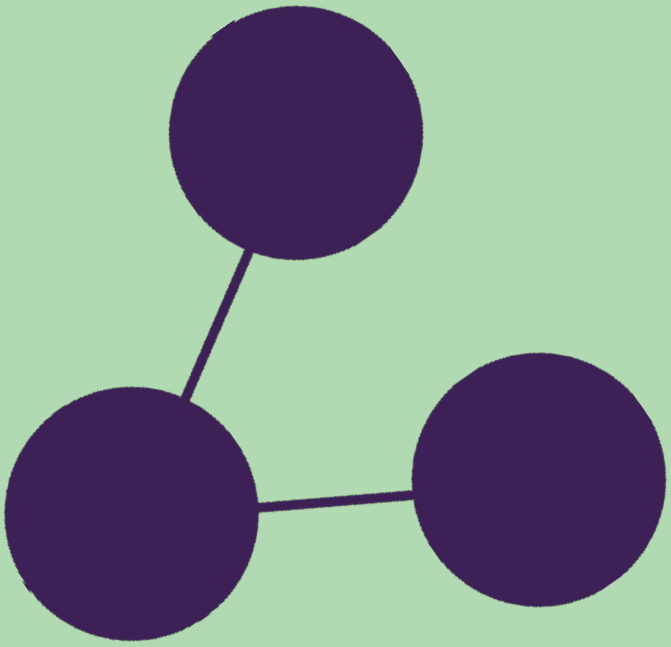
evelon

DIN GUIDE TIL DAGENS OG FREMTIDENS IT-SIKKERHET

– Vi har en manglende bevissthet og kultur i det norske samfunnet som det tar tid å endre. Vi undervurderer både den faren vi som enkeltmennesker blir utsatt for, og faren for store angrep mot systemene våre, uttalte statssekretær Thor Kleppen Sættem (H) i Justisdepartementet til NTB. Sikkerhetsmangler i dagens virksomheter er i stor grad resultat av utilstrekkelig kunnskap om trusselbildet, og at ledelsen ikke har kunnskap om hvilke tiltak som behøves.

Dagens trusselbilde krever kontinuerlig sikkerhetsarbeid med god forankring på alle nivå i virksomheten. Tidligere har man i sikkerhetsarbeidet ofte fokusert på å bygge murer for å skille virksomhetens utside fra innside. Digitaliseringen har endret måten vi jobber på og det er derfor blitt stadig mer vanlig å innrette seg etter rettigheter basert på roller og identiteter. Sikkerhet handler i tillegg i stor grad om håndtering av integritet og personopplysninger, som i det siste har fått økt fokus på grunn av GDPR. I dag er det ikke tilstrekkelig å sette opp en sikker løsning og nøye seg med det. Ingen kan garantere absolutt sikkerhet, men det er mulig å iverksette flere tiltak for å øke beskyttelsen og dermed gjøre det vanskelig og ressurskrevende for potensielle angripere å påføre virksomheten skade.

En pålitelig skyleverandør er en verdifull partner i kampen mot cybertruslene. I denne e-guiden forklarer vi hvordan du legger en strategi og velger riktig partner



43%
av alle cyberangrep er rettet mot små bedrifter.

evelon

SLIK BEGYNNER DU REISEN MOT ET SIKKERT IT-MILJØ

Sikkerhet er et samspill mellom deg som kunde, dine ansatte og dine leverandører. Skytjenesteleverandørens ansvar er å levere infrastruktur og tjenester ifølge avtalen, mens din jobb er å forstå trusselbildet og konsekvensene av sikkerhetsbrudd. Dette innebærer at du blant annet må ta en nøye vurdering av leverandøren, bestille de rette tjenestene (ofte en sammensetning av standardiserte og tilpassede) og – ved behov – gi instruksjoner på utførelsen.

Målet er å gjøre det så vanskelig som mulig for den cyberkriminelle å komme seg inn i virksomhetens systemer. Det er viktig å ha rutiner og ressurser på plass for snarlig å kunne håndtere og spore de sikkerhetsbrudd som skjer. Ingen systemer er helt sikre, og det er derfor viktig å tenke sikkerhet i all ledd og på alle nivåer. Velg tjenester, produkter og servicenivå som gjør det enkelt for dine ansatte å handle i tråd med virksomhetens sikkerhetspolicy. Husk at det skal være lett å gjøre rett.

Det finnes flere viktige trinn på veien mot å velge rett strategi for IT-sikkerhet og i dette arbeidet kan en IT- partner tilby verdifull veiledning. Bruk gjerne problemstillingene i dette dokumentet som underlag for en samtale.

41%

De vanligste konsekvensene av sikkerhetsbrudd er tapte arbeidstimer (41%) og tapt data (16%).

evelon

KARTLEGG DAGENS SITUASJON OG BEHOV I EN SIKKERHETSANALYSE

Ledelsen må ha kunnskap om hva som bør beskyttes, samt konsekvensene av ulike hendelser relatert til sikkerhet. Derfor kan det for mange være behov for å foreta en sikkerhetsanalyse. En slik analyse vil gi et godt utgangspunkt for å bygge et sikkert miljø, som både oppfyller virksomhetens krav til funksjon og minsker sårbarheten rundt det som er viktig å beskytte. Nedenfor følger forslag til steg i analysen:

1. Identifiser hva dere har som bør beskyttes
Hvilken type informasjon har dere som er av interesse for tredjeparter? Det kan være alt fra kredittkortopplysninger til bedriftshemmeligheter. Klassifiser virksomhetens informasjon med verdier for hvilket beskyttelsesbehov som er ønskelig.

2. Utfør en konsekvensanalyse
Vurder hvilke konsekvenser det vil få for virksomheten dersom noen for eksempel får tilgang til høyt konfidensiell informasjon, eller hvis en virksomhetskritisk applikasjon er nede eller blir stengt et visst antall minutter, timer eller dager. Ta i tillegg hensyn til lover og forordninger der virksomheten risikerer bøter ved overtredelse. Regn på hva de ulike konsekvensene vil innebære av kostnader og tapte inntekter for virksomheten. Ta stilling til hvilke konsekvenser dere kan leve med og hvilke som er uakseptable.

3. Identifiser sårbarheten
Forsøk og analyser virksomhetens miljø gjennom øynene til en cyberkriminell. Hvor finnes det potensielle sikkerhetshull? Kan dere for eksempel verifisere at kun godkjente brukere har tilgang?

4. Finn ut hvordan truslene ser ut og hvor de kommer fra
I kartleggingen av potensielle trusler kan det være lurt å stille spørsmålet om hvem som kan ha til hensikt og evner å gjennomføre et angrep mot deres virksomhet. Kriminelle på nettet handler ut fra en rekke ulike motiver. Det kan være for å skaffe innsikt i verdifull informasjon for å sabotere, eller for å oppnå økonomisk vinning.

Malware, hendelser forårsaket av ansatte, sosial manipulering (phishing) og forsøk på datainnbrudd (hacking) er de vanligste formene for sikkerhetshendelser med henholdsvis **20%, 10%, 8% og 8%.**

evelon

FORTS>

Det er verdt å merke seg at truslene også kan komme innenfra virksomheten. Det kan for eksempel være i form av illojale medarbeidere, eller ved at medarbeidere utsetter organisasjonen for risiko på grunn av ubetenksomhet. Eksempler på sistnevnte kan være at en ansatt benytter seg av private enheter som ikke er sikret for å utføre virksomhetsrelatert arbeid.

5. Utarbeid rutiner for oppfølging og ansvar
Når et sikkerhetsbrudd finner sted gjelder det å ha rutiner som gjør at angrep raskt oppdages og rettes. Det er i tillegg viktig å ha god sporbarhet slik at det er mulig å gå tilbake for å analysere årsaken til sikkerhetsbruddet. Det kan være lurt å ha en dedikert sikkerhetsansvarlig internt i virksomheten, som blant annet har ansvar for at katastrofeøvelser gjennomføres, at virksomheten har nødvendig backup, samt vet hvilken hjelp eller hvilke ressurser som kan kalles inn på kort varsel.

6. Eliminer sårbarheter
Arbeidet med å eliminere sårbarheter kan gjelde det fysiske miljøet, spesiell sensitiv informasjon eller teknologiske løsninger. Et annet eksempel på sårbarhet er ansattes atferd. Det kan klikkes på en skadelig lenke eller brukes en privat mail eller lagringstjeneste til virksomhetsinformasjon. Gode tiltak vil være å sørge for at virksomhetens IT-miljø er funksjonelt nok til at ingen lokkes til å bruke usikre tjenester på nettet, i tillegg til å ha verktøy på plass som sikrer begrensede konsekvenser dersom noen klikker på en skadelig lenke eller åpner et skadelig vedlegg. Andre sårbarheter det kan være verdt å tenke på:

- ✓Password og måten de blir beskyttet og oppbevart på
- ✓Mistede/frastjålet enheter

Ansiktsgjenkjenning eller kodelås burde være obligatorisk på alle enheter med virksomhetsdata. Tofaktorautentisering er et nyttig verktøy for å minske risikoen for alvorlige konsekvenser ved inntrufne sårbarheter. Det innebærer at den som skal få tilgang til en tjeneste, må verifisere seg med to metoder; både ved hjelp av passord og verifisering med en kode som man får på SMS/opplest over telefon.

Virksomheten kan i tillegg bestemme ulike sikkerhetsnivåer på forskjellig type data basert på behov. Det går for eksempel an å sette opp rettighetsstyring, hvor det er mulig å begrense tilgangen til enkelte samarbeidsflater og dokumenter. Dette er med på å redusere risikoen for at ansatte lagrer informasjon på feil sted, eller sender sensitive dokumenter via e-post.

GDPR

Dagens personvernlovgivning bygger på et EU-direktiv fra 1995 – da faksmodemer var moderne og smarttelefoner ennå ikke var oppfunnet – og den er foreldet på flere områder. GDPR (General Data Protection Regulation) er EUs forordning for personvern, som 1. juli 2018 skal erstatte det vi i dag kjenner som personopplysningsloven. Formålet med de nye reglene er å sørge for god beskyttelse og håndtering av personopplysninger.

Personopplysninger er data som kan knyttes til deg som person, for eksempel navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer).

GDPR stiller strenge krav til dokumentasjon av rutiner, behandling av personopplysninger, sikring av opplysninger og risikovurdering. Bøter ved brudd på bestemmelsene skal fastsettes etter overtredelsens grovhet - og hvilke sikringstiltak virksomheten har iverksatt. For alvorlige brudd på den nye loven kan virksomheter risikere å få en bot på opptil 4% av konsernets årlige omsetning, eventuelt 20 millioner Euro dersom dette utgjør en større sum.

For mindre alvorlige brudd kan boten utgjøre opp til 2% av årlig konsernomsetning, eller 10 millioner Euro - også her vil virksomheten måtte betale alternativet med størst totalsum. Det er Datatilsynet som er ansvarlige for å kontrollere at GDPR overholdes etter innføringen.

evelon

GDPR – 8 TIPS TIL HVORDAN DIN VIRKSOMHET KAN KOMME I GANG

1. Skaff dere en skriftlig oversikt over hvilke personopplysninger dere behandler (samler inn, bruker, lagrer), samt hvor og hvordan disse dataene behandles. Husk at selv om dere bruker databehandlere (for eksempel leverandører av drift- og skytjenester) er dere fortsatt behandleransvarlig.

2. Gjennomfør og dokumenter en risikovurdering av behandlingen av personopplysninger i virksomheten. Skaff dere oversikt over regelverket, og finn ut hvilke plikter som gjelder for deres virksomhet. Virksomheten må utvikle skriftlige rutiner for gjennomføring av de rettighetene som ligger til privatpersoner i regelverket.

3. Skaff dere teknisk innsikt og finn ut om personvernet ivaretas av virksomhetens nåværende IT-løsning, eller eventuelt hva som må gjøres for å sikre en tilfredsstillende løsning.

4. Få på plass skriftlige rutiner for internkontroll og tiltak for å overholde de nye pliktene. Sørg i tillegg for at alle ansatte følger de nye rutinene når reglene trer i kraft. Lag en forståelig personvernerklæring som sier noe om hvordan virksomheten behandler personopplysninger.

5. Avklar roller og ansvar og ikke minst bygg relevant kompetanse. Dersom det foreligger en risiko knyttet til personvern, må virksomheten også utrede hvilke personvernkonsekvenser risikoen kan ha.

6. Sørg for at virksomheten har innebygd personvern. Dette vil si at personvern er ivaretatt i forhold til nye tiltak og systemer.

7. Finn ut om virksomheten må ha en personvernrådgiver. En personvernrådgiver er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet.

8. Gjør dere kjent med:
- Den enkeltes rett til å kreve at personopplysninger slettes («retten til å bli glemt»)
- Den enkeltes rett til å kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et kjent filformat («dataportabilitet»)
- Den enkeltes rett til å motsette seg profilering
- Regelen om at alle henvendelser fra privatpersoner relatert til personopplysninger skal besvares innen en måned

evelon

ANBEFALTE STEG MOT SIKRE TJENESTER I SKYEN

Spørsmålet er ikke lenger om skyen eller skytjenester er sikre. I dag handler det om å velge riktige tjenester som oppfyller virksomhetens nåværende og fremtidige krav til sikkerhet, tilgjengelighet og regeletterlevelse. I tillegg er det mye dere som virksomhet kan gjøre for å sikre deres data:

1. Innled sikkerhetsarbeidet med å utføre en grundig sikkerhetsanalyse. Sørg deretter for at utfallet av sikkerhetsanalysen og strategien fremover forankres i ledergruppen. Dette er noe en IT-leverandør kan bidra med, dersom virksomheten ikke besitter denne kompetansen selv.

2. Velg deretter skystrategi, tjenester og eventuelt skyleverandør ut fra dagens og fremtidens krav til sikkerhet, integritet, tilgjengelighet og regeletterlevelse. Det er viktig å finne den rette balansen mellom sikkerhet og fleksibilitet slik at ansatte ikke opplever at det settes begrensninger ved implementasjon av nye tjenester.

3. Lær de ansatte grunnleggende IT-sikkerhet. Det er helt essensielt for virksomheter å hjelpe de ansatte til å beskytte virksomhetens data. Dette kan for eksempel gjøres ved å holde sikkerhetskurs hvor det blir vist hvordan de enkelt kan se om et vedlegg eller en link er skadelig. Det er i tillegg lurt å lage en intern sikkerhetspolicy som sier noe om hvor og hvordan de ansatte skal lagre dokumenter som inneholder personsensitive og virksomhetskritiske data.

4. Trusselbildet endres med tiden, og det vil stadig komme nye sikkerhetstrusler. Sørg derfor for å etablere prosesser for et dynamisk og kontinuerlig sikkerhetsarbeid.

evelon

OPPSUMMERING

Virksomheter kan bli utsatt for både interne og eksterne trusler. Det kan enten være organisasjoner eller hackere med økonomiske og ideologiske motiver, eller illojale eller uheldige medarbeidere som kan forårsake alvorlige informasjonslekkasjer.

Dagens virkelighet er at trusselbildet er i stadig endring og at antall cybertrusler øker i omfang og antall - selv for mindre bedrifter. Det er ikke lenger tilstrekkelig å sette opp en "sikker løsning" og håpe på det beste – sikkerhetsarbeidet må være en pågående prosess som gjennomsyrer virksomheten på alle plan.
GDPR gjør at samtlige virksomheter er nødt til å sette IT-sikkerhet på agendaen. Ved å implementere en moderne skyløsning kan også de minste virksomhetene få tilgang til bransjeledende sikkerhetsløsninger, uten å måtte bekoste en stor IT-avdeling.

evelon

Kilder

Personvernforordningen (GDPR)

FRA Årsrapport 2016

Den svenske myndigheten for samfunnsvern og beredskap:
Informasjonssikkerhet - trender 2015

Symantec ISTR Financial Threats Review 2017

Symantec ISTR Special Report: Ransomware and Businesses 2016

2015 Trustwave Global Security Report

Akenine, Daniel: Välkommen GDPR!

Nilsson, Tomas: Cyberhoten ökar i finansvärlden

F-Secure Business Security Insider: ID-kapning är en växande plåga

Harvard Business Review, January-February Issue 2016: Collaborative Overload

Strategic Analytics: Global Mobile Workforce Forecast, 2015-2020, November 2015

Small Business Trends: CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know, Jan. 3, 2017

https://www.pressreader.com/norway/dagsavisen/20180313/281784219611459

evelon

KONTAKT OSS

Avdeling Lillevik IT
Brynsalléen 4
0667 Oslo

21 41 50 00

Avdeling Bridge IT
Strømtangevegen 11A
3950 Brevik

35 03 20 00

Avdeling IMEMO
Åslyveien 15
3170 Sem

91 34 63 66

Chat med oss
www.evelon.no

Send en e-post
salg@evelon.no

evelon