CORPORATE SECURITY

2. utgave – September 2012

Er du en av de få som har en plan?

Under halvparten av Norge AS har en beredskapsplan mot det utenkelige. – Fremtiden er bekymringsfull, mener Shazhad Rana (t.v.), Vibeke Hammer Madsen og Kristine Beitland.

broddcommunication

Forenklet hverdagen med nettskyen

Norway Seafoods lar nettskyen ta seg av alt fra backup til antivirus. Det har forenklet deres hverdag.

KRISTINE LØWE, redaksjonen@broddcom.no

Roar Steffensen, IT-sjef for Norway Seafoods i Norge, forteller at han opplevde det som en positiv overraskelse, da han begynte å bevege seg inn i skytjenestene. –Jeg ble overrasket over alle mulighetene som fantes. Det har forenklet hverdagen.

Hans råd til bedrifter som vurderer nettskytjenester er at det lønner seg å være litt nysgjerrig: Vær sunt skeptisk, men ikke for skeptisk. – Vi må ha et edruelig forhold til sikkerhet. Det skal være så sikkert som mulig, men det skal jo også være praktisk. Der har vi vurdert og analysert for og imot for alle skytjenestene vi bruker i dag, sier han.

I dag har Norway Seafoods et bredt spekter av funksjoner ivaretatt av nettskytjenester, og de utvider det stadig. Blant annet har de deler av sin kritiske backup der. I tillegg til å bruke offentlige, abonnementsbaserte skytjenester, benytter selskapet seg også mye av en privat nettsky. Hele plattformen deres – økonomi, administrasjon osv. – ligger på sistnevnte.

Sjekker leverandørene i brukerforum

I en offentlig nettsky bruker selskapet utelukkende betalte løsninger, en blanding av norske og amerikanske selskaper.

– I vurderingen av potensielle nye leverandører av nettskytjenester, er Google en nyttig venn. Å bruke litt tid på å sjekke forskjellige forum om andre har erfaringer med tjenesten eller leverandøren er også viktig. Jeg ber alltid om en presentasjon av løsningen for å se hvordan den henger sammen i vurderingen av en ny leverandør eller tjeneste. Deretter bruker jeg litt tid på nettet for å sjekke referanser og andres erfaringer. Hvis noen har negative erfaringer, er jeg selvsagt veldig interessert å lese om det, påpeker han.

En tjeneste han er spesielt fornøyd med er en antivirus-/antimalware-løsning som er nettskybasert. Den gjør at selskapet slipper å ha servere på huset for å håndtere antivirus, og klienten tar liten plass og krever lite ressurser, og ikke minst – den gjør jobben.

– Det er en helt suveren tjeneste som gjør alt fra nettleseren. Nå som stadig flere tjenester blir tilgjengelig i skyen, må man oftere tenke over om man skal kjøre det hele fra skyen eller sette opp tjenesten på huset. Sistnevnte krever ofte mer ressurser internt, mens i nettskyen overlater du det meste til leverandøren. Det gjør at vi kan bruke mer ressurser på å understøtte det forretningskritiske, forklarer han.

Mener leverandørene prioriterer sikkerhet

Men sikkerhet er alltid en prioritet for selskapet, som må kunne stole på at deres data blir ivaretatt og ikke kommer på avveie – eller at uautoriserte får tilgang.

– Mitt generelle inntrykk er at dette blir prioritert hos leverandørene av slike tjenester. Det finnes jo alltid historier der man hører at her og der har det vært innbrudd, og at data kan ha havnet på avveie, men vurderer man å ta i bruk nettskytjenester, må man vurdere nøye om et potensielt data–innbrudd, og i verste fall datatap, vil være skadelig for bedriften og eventuelle andre konsekvenser av dette. I noen tilfeller vil svaret si seg selv, men jeg er av den absolutte oppfatning at leverandører i dette segmentet i økende grad fokuserer på sikkerhet, sikker lagring og tilgang. Dette åpner flere og flere muligheter for oss som skal levere IT-systemer for å understøtte forretningen. Det er ikke nødvendigvis lenger slik at det vi gjør på huset, er det beste i alle tilfeller, påpeker han.

Men den menneskelige delen av IT-sikkerhet må Norway Seafoods fortsatt jobbe med:
– Det er alltid en konflikt, Brukeren vil ha enkelhet mens IT vil ha det sikkert, avslutter Steffensen.

Vi må ha et edruelig forhold til sikkerhet. Det skal være så sikkert som mulig, men det skal jo også være praktisk.

Roar Steffensen, IT-sjef for Norway Seafoods i Norge

THE WORLDS FASTEST, LIGHTEST, EASIEST-TO-MANAGE ENDPOINT ANTIVIRUS PROTECTION

- Instantaneous Cloud-Predictive Malware Protection
- 700 KB Client: Installs, Scans & Protects In Seconds
- Doesn't create conflicts - even with other endpoint security products
- Simple, Feature-Rich Web-Based Management Console
- Powerful Agent Commands, including Rollback
- Instantaneous Global Support & Remediation

PROTECTS AGAINST:
VIRUSES,
SPYWARE,
WORMS,
ROOTKITS,
KEYLOGGERS,
TROJANS,
ADWARE

WeCloud
PEACE OF MIND IN EVERY CONNECTION

WeCloud er distributør av Webroot® SecureAnywhere™ Business - som strategisk Webroot partner i Skandinavia, og er eksperter på IT-sikkerhetstjenester levert i skyen.
Kontakt oss på info@wecloud.no eller www.wecloud.no

WEBROOT®
SecureAnywhere. Business

Secure Web Access through the Cloud

zscaler®

- Integrated Web- & Email Security as a Service
- Advanced Threat Detection
- URL-Filtering & Web 2.0 Control
- Bandwidth Management
- Data Loss Prevention
- Real time Reporting

Zscaler Web Security Cloud Service gir sikker og kontrollert nettilgang. På alle lokasjoner og for alle ansatte, hvor som helst, på hvilken som helst enhet: For PCer, bærbare datamaskiner, nettbrett og smarttelefoner. Kostnadseffektiv sikkerhet for virksomheter av alle størrelser. Ingen hardware eller software: Alltid up-to-date sikkerhet i skyen!

The Cloud Security Company
www.zscaler.com

WeCloud
PEACE OF MIND IN EVERY CONNECTION

WeCloud er strategisk Zscaler partner i Skandinavia, og er ekspert på IT-sikkerhetstjenester levert i skyen.
Kontakt oss: info@wecloud.no Info: www.wecloud.no

SPØRSMÅL TIL PANELET corporate security	RIKARD ZETTERBERG VD, WeCloud AB	TERJE WOLD Adm. Dir. Invenia	OLE KRISTIAN MÅLBAKKEN Security Consultant, Secode
Hvor ligger de største sikkerhetsutfordringene i Norge AS?	**Den største** sikkerhetsutfordringen i Norge ligger i å identifisere og implementere et felles sikkerhetsnivå for alle enheter og systemer i virksomheten. Den ekstreme økning av antallet mobile enheter, også mangfoldet av operativsystem, som behandler virksomhetssensitiv informasjon har gjort det vanskligere å opprettholde sikkerhetsnivået i hele virksomheten.	**Norge er** et informasjons- og kunnskapssamfunn der stadig mer av verdiskapingen er intellektuell kapital, immaterielle verdier og informasjon. Utfordringen blir da å ivareta god informasjonssikkerhet og forebygge økende datakriminalitet. Mange ledere svikter her sitt ansvar, overser utviklingen eller forstår ikke alvoret. Både samfunnskritisk infrastruktur og store bedriftsverdier står på spill her.	**De største utfordringene** er manglende bevissthet og forståelse for risiko knyttet til informasjonsverdier og tjenester. I den grad risiko vurderes og håndteres i offentlige og private virksomheter, vil det også være lite samsvar mellom risikoperspektiv på ledelsesnivå og operativt nivå. Dette skyldes manglende bevissthet og manglende kommunikasjon om risikoer på de forskjellige lagene i virksomhetene. Grunnen til dette kan igjen skyldes et lite tilgjengelig begrepsapparat og naivitet i forhold til hva trusselutøvere faktisk kan utrette av skade.
Hvordan vil trusselbildet endre seg de to neste årene?	**Vi kommer å se en økning** på antall unike skadelige koder som ikke blir fanget opp av de tradisjonelle beskytelsene vi bruker i dag. Den raskest voksende kanalen for nye skadelige koder er i dag http/https der trusselbildet er plattform uavhengig. Web lesere i smarttelefoner og nettbrett er langt mer sårbare enn weblesere vi bruker på datamaskiner, så vi kan vente oss en økning av angrep mot de mobile enhetene.	**Trusselbildet vil forverre seg** og sikkerhetsrisikoen øker. Når FBI sier at "cybertreats" snart er en større trussel enn terrorisme, sier det alt. Det samme skjer i Norge. Dataangrepene vil bli flere og mer avanserte, og stadig flere bedrifter rammes. Problemet er at samfunnet ikke tar dette inn over seg, og bedriftene henger etter i kunnskap, kultur og utøvelse av god informasjonssikkerhet.	**Vi vil se en økning** av trusler som påvirker enkeltpersoner og forretningsvirksomheter. Det utvikles stadig mer sofistikert ondsinnet programvare (trojanere) for å tappe informasjon som benyttes ifm ID-tyverier og forretningssvindel. I tillegg gjør vi oss ekstra sårbare for disse truslene ved at vi stadig krever økt fleksibilitet og tilgangsmuligheter fra våre egne mobiltelefoner og nettbrett (BYOD). Sensitive personopplysninger og virksomhetskritisk informasjon lagres også på servere operert av ukjente, og i land med få eller ingen krav til sikring av slike opplysninger.
Hva skal til for at toppledelsen skal se på sikkerheten som en investering og ikke en kostnad?	**Gjennom å synliggjøre** nytten og besparingen virksomhetens eksisterende sikkerhetsløsninger gir, får du lettere gehør for å fortsette sikkerhetsarbeidet og dekke behovet for å holde seg oppdatert på nye trussler og løsninger. Analyser f.eks noen av de seneste kjente angrep som intreffer hos sammenlignbare virksomheter og hvordan det har påvirket deres IT miljø.	**De kriminelle** knuser ikke lenger ytterdørene. De er i stedet innenfor brannmuren uten at bedriftene merker det. Mange ledere bråvåkner da til store kostnader og omdømmetap. Det hele må snus til en proaktiv investering i sikkerhet med årvåkent lederansvar, god sikkerhetskultur og vedvarende satsing. Det kan gi økt konkurransekraft og er god forvaltning av selskapet slik bl.a. aksjeloven krever.	**Ledelsen bør ta en kritisk** gjennomgang av verdiene som deres informasjon og tjenester representerer. Deretter bør de stille seg selv spørsmål om hvordan deres virksomhet vil bli påvirket hvis denne informasjonen eller disse tjenestene går tapt eller blir utnyttet i vinnings hensikt eller for å skade. Svarene bør formidles i hele organisasjonen for å sikre at alle jobber mot samme mål om å sikre virksomhetens omdømme og fremtidige forretningsmuligheter – investere i sin egen arbeidsplass!
Investerer norske virksomheter nok i sikkerhet?	☐ JA ☑ NEI	☐ JA ☑ NEI	☐ JA ☑ NEI
Finnes det tilstrekkelig sikkerhetskompetanse blant medarbeidere?	☐ JA ☑ NEI	☐ JA ☑ NEI	☐ JA ☑ NEI
Burde virksomheter benytte sikkerhet i sitt omdømmearbeide?	☑ JA ☐ NEI	☑ JA ☐ NEI	☑ JA ☐ NEI