

Sikkerhetsarkitektur

En sikkerhets-arkitektur? Holder det ikke om vi har en nettverksarkitektur og kanskje en systemarkitektur? Begrepet er ikke ukjent for Mellvik-Rapportens lesere, som også vet hvor viktig det er å være på høyde med hensyn til sikkerhet. Poenget i denne sammenhengen er at våre omgivelser forandrer seg. VPN+SSL-kombinasjonen som vi diskuterer i artikkelen ovenfor er et godt eksempel. Videre kan vi brenne av utrolige penger og andre ressurser uten å få nevneverdig sikkerhet igjen for pengene – om vi ikke har både oversikt og innsikt.

Slik verden rundt oss ser ut i dag, har vi ikke annet valg enn å ta ansvaret selv (se margrammen nedenfor). At vi kjøper hjelp fra tilgjengelig ekspertise forandrer ikke det faktum at vi fortsatt sitter med ansvaret, og derfor må ha både oversikt og grunnleggende innsikt.

Nettopp oversikt står i fokus i denne artikkelen. Vi gjennomgår en samling overordnede punkter, elementer og regler hvorav et varierende antall må være med i *din* sikkerhetsplan – som er et mindre vidløftig navn på en sikkerhetsarkitektur. En slik plan hører naturlig hjemme som del av en moderne nettverksarkitektur, som vi diskuterte i en egen artikkelserie i første halvår.

En plan for god sikkerhet

Følgende elementer kan inngå i en overordnet sikkerhetsplan:

- ✓ Risiko- og trussel-analyse
- ✓ Regler (policy) og rutiner
- ✓ Fysisk sikring, bevisstgjøring av medarbeidere
- ✓ Sikring av protokoller, applikasjoner og tjenester
- ✓ Kryptering, autentisering
- ✓ Sikring av nettverkets yttergrenser
- ✓ Sikring av fjernaksess

Trenger du en sikkerhets-arkitektur?

Kanskje ikke, men sannsynligheten er stor for at du gjør det – enda. I en ikke altfor fjern fremtid – som burde ha vært her for lenge siden – blir hele problemstillingen et leverandøransvar. Objektivt sett er det ingen grunn til at virksomheter flest skal ha sikkerhetsekspertise eller ansvar for egen IT-sikkerhet. Sikring er krevende og forutsetter en grad av ekspertise primært store miljøer er i besittelse av. Dette er hovedårsaken til at et altfor beskjedent antall norske Internett-tilknyttede virksomheter har skikkelig sikring. Faktum er at å bygge opp egen sikkerhetsekspertise for de fleste organisasjoner er bortkastede ressurser.

Lite nytter det imidlertid å ønske seg til en annen situasjon. Markedet, og spesielt leverandørsiden, mangler modning og er ikke i stand til å levere det kundesiden trenger. Så underlig det kan høres, har ikke engang store og antatt profesjonelle Internett-leverandører et fornuftig tilbud for sikkerhetsstyring og -ansvar å tilby til sine kunder. Små og kunnskapsrike aktører rører seg i periferien, men har ikke verken ressurser eller tyngde til å dekke behovene. Mange av dem er rene produkt/tjeneste-leverandører, hvilket er verdifullt og nødvendig, men ikke tilstrekkelig. Behovet for virksomheter flest er ikke på produkt-, teknologi- og konsulent-nivå, men på tjenester og ansvar.

Der står vi, og må inntil videre ta ansvaret selv. Det er – som vi var inne på ovenfor – krevende, men slett ikke umulig.

Trusselanalyse

En grundig trusselanalyse kan lett bli en komplisert og tidkrevende prosess, blant annet fordi spekteret som skal dekkes er formidabelt. Analysen forenkles hele tiden ved å inkludere risiko som en kvalifiserende faktor. Mens det er trusler vi skal beskytte oss mot, er det også innlysende at en trussel alene ikke er nok til å representere risiko. Og til slutt er det

risiko som kvalifiserer beskyttelsestiltak. Vi diskuterte dette forholdet i artikkelen om hypersikring i Mellvik-Rapporten nr. 102, og presenterte blant annet følgende høyst relevante ligning:

$$\text{risiko} = \text{trussel} * \text{sårbarhet} * \text{hyppighet}$$

Med dette forholdet i mente, er en tabelloppstilling den mest effektive måten å analysere og systematisere trusler på. I tabellen inngår potensielt truede objekter (tjenere, klienter, programvare, data etc.) langs den ene akse, og de mulige truslene langs den andre. Både objekter og trusler kartlegges i en forutgående analyse, og grupperes på en måte som synes rimelig under omstendighetene.

Den resulterende oppstillingen kan se ut som tabellen nedenfor, der vi kan benytte bokstavkoder eller tallkoder for å vektlegge de ulike kombinasjonene. Sørg for å finne vekt tall som er riktige for nettopp din organisasjons prioriteringer dersom du velger tall som til slutt skal summeres.

Tabell 1 Matrise for trusselanalyse (eksempel). I kryssningspunktene graderes konsekvensene og sannsynligheten for at kombinasjonen skal inntreffe.

Konsekvens/ sannsynlighet	Brukerutstyr	Tjenere	Nettverks- utstyr	Programvare	Tjenester	Data
Ikke-autorisert tilgang	B/A ^a	B/B	C/B	A/B	B/C	A/B
Lekkasje (ikke-autorisert innsyn i gradert materiale)	B/C	B/B	C/C	A/B	B/C	A/B
Utilgjengelighet (denial of service)	B/B	B/B	B/B	B/B	B/B	D/D
Mykskade (korrumpert)	A/C	B/C	C/C	A/B	D/D	A/B
Virus	B/B	B/B	B/B	B/B	B/C	D/D
Tyveri	A/D	B/D	B/D	A/B	C/C	A/B
Fysisk skade	A/D	B/C	C/C	D/D	D/D	D/D

^a Konsekvens: A=destruktiv, B=alvorlig, C=hemmende, D=uvesentlig. Sannsynlighet: A=meget høy, B=høy, C=beskjeden, D=minimal.

Når tabellen er fylt ut og innholdet kvalitetssikret, er neste punkt å bestemme hvor smertegrensen går. Hvilke trusler er viktige nok og store nok til å gripes fatt i? Husk at verdien av det som skal sikres, er den viktigste målestokk for hvor mye penger og andre ressurser vi kan bruke på en gitt trussel. Er for eksempel ethvert driftsavbrudd uakseptabelt, er det innlysende at alle tabellfelter med konsekvens høyere enn D må gripes fatt i.

Regler og rutiner

Sikkerhetsregler skal definere og dokumentere hvordan våre systemer og verktøy kan brukes med minimal risiko. Det bør utarbeides både overordnede regler og utstyrs/verktøy-spesifikke regler. Overordnede regler spesifiserer virksomhetens grunnleggende filosofi, for eksempel at alt som ikke er eksplisitt tillatt, skal ansees som forbudt – eller motsatt.

Reglene skal være enkle, klare og kunne håndheves (se rammen nedenfor). Videre skal de fortelle om ansvar, overvåking, tilgang, konsekvenser og henviser til prosedyrer/rutiner.

Følgende områder bør være dekket av egne eller kombinerte regelsett:

- ✓ Fysisk sikkerhet
- ✓ Sikring av brukerutstyr
- ✓ Programvare (applikasjoner og verktøy, operativsystemer)
- ✓ Sikring av tjenere og andre sentrale ressurser
- ✓ Fjernaksess, kryptering, autentisering
- ✓ Adressering og ruting i nettverket
- ✓ Trådløse nettverk
- ✓ Brannmurer, grenser mellom interne og eksterne nettverk

I rammen på neste side og tilsvarende rammer i neste utgave diskuterer vi forhold knyttet til sikkerhetsregler innen spesifikke områder – som epost, bærbare maskiner, trådløse nettverk, og ikke minst henvisninger til nettressurser som er spesielt interessante i forbindelse med policy-arbeid.

Sikringsmekanismer

Vi har ved en rekke anledninger diskutert det ofte neglisjerte forholdet mellom sikringstiltak og medarbeidere (opplæring/holdninger). Enhver

sikkerhetsarkitektur inkluderer derfor en plan for hvordan brukerne både skal bevisstgjøres og holdes oppdatert med hensyn til sin egen rolle i sikringsarbeidet. Artikkelen “En sikkerhetsbevisst organisasjon” i Mellvik-Rapporten nr. 78 gir en detaljert oppskrift på hvordan en slik prosess kan gjennomføres.¹⁰

Uten mekanismer blir det imidlertid ingen reell sikkerhet. Hvilke vi vektlegger og hvordan de skal brukes er selvsagte ingredienser i vår plan: Fysisk sikring, nettverkssikring, systemsikring, klientsikring, applikasjonssikring og

Det er klart vi har en sikkerhets-policy...

Det er en stund siden sikkerhet kom som en ‘attpåklatt’ – dersom vi fikk tid. Sikkerhet er som regel med fra begynnelsen av. Det koster – penger og tid, og resultatet er ofte lite synlig. Vi skal ende opp med en følelse, en velbegrunnet følelse – av trygghet. Derfor er det fortsatt fra tid til annen vanskelig å få satt av tilstrekkelige ressurser til sikkerhetsarbeidet. For eksempel til vår **sikkerhetspolicy**.

La oss anta at den finnes, den har eksistert en stund, er kanskje ferdig, presentert og godkjent, eller halvferdig – fortsatt ‘underveis’. Uansett hvilken status den måtte ha, er følgende huskereglene nyttige for det videre arbeidet:

- **Er punktene korte nok?** Lange og omstendelige punkter blir verken lest eller husket, og kan være vanskelige å håndheve. Hele policy-dokumentet skal være på mindre enn 3 sider. Bli det mer, er innholdet trolig mer prosedyrer og veiledninger enn policy.
- **Er punktene lettfattelige?** Dette er ikke stedet for runde formuleringer eller antydninger. ‘Rake pucker’ er det eneste som teller – for eksempel: “Nedlasting og/eller videreformidling av musikk, film eller annet kopibeskyttet materiale tillates ikke.” Brukerne liker klarhet, ulne formuleringer skaper usikkerhet og diskusjon.
- **Er det mulig?** En regel som ikke er gjennomførbar eller lar seg håndheve, er ikke verdiløs, men skadelig. “Brukere må ikke laste ned virus” høres fint ut, men hvordan skal det håndheves? Likeledes har de fleste regler økonomiske konsekvenser som i noen tilfeller viser seg å være utenfor rekkevidde. Eksemplet med virus hører også til denne gruppen. Å håndheve regelen kan være mulig, men altfor kostbart uansett miljø. Med hensyn til virus er riktig vinkling å angi hvilke kontrolltiltak som gjelder og hvilke restriksjoner som gjelder for brukerne.

Før en policy settes ut i livet, er det en god idé å ‘prøvekjøre’ den på en håndfull tilfeldig valgte brukere. Forvent ikke at de skal like den eller synes den er god, men finn ut hvordan de reagerer. Tilbakemeldinger som ‘dette er bare tull’ er ikke akseptable, men må følges av årsaker og forklaringer på hva som er galt. Dersom brukeren forstår viktigheten av sikring og sin egen rolle i bildet, er vi allerede et godt stykke på vei.

¹⁰ Savner du denne utgaven? Send epost til mr@mellvik.no med referanse til ditt abonnentnummer (eller navnet abonnementet er registrert på), så sender vi artikkelen i pdf-format.

så videre. På samme måte som for nettverksarkitektur kontra design, skal sikkerhetsarkitekturen fortelle hva og hvorfor, mens en tilhørende implementasjonsplan går i detalj med hensyn til produkter, verktøy og konfigurasjoner. Blant annet bør følgende områder/teknologier være dekket i den forbindelse (overordnet, implementasjon og policy):

- ✓ Brannmurer og DMZ
- ✓ Proxyer
- ✓ VPN, autentiserings-protokoller og -mekanismer (for eksempel PKI)
- ✓ Nettverksadministrasjon, bruk og sikring av SNMP
- ✓ Installasjon og konfigurasjon av trådløst utstyr
- ✓ Sikring av DNS, LDAP og andre høynivå-protokoller

En plan

Med ingrediensene på plass skulle vi tro sikkerhetsplanen kan ferdiggjøres – og ofte er det slik det foregår. Erfaring tilsier imidlertid at et siste trinn er nyttig. En sluttkontroll eller kvalitetskontroll – en kritisk gjennomgang av innholdet, der vi stiller spørsmål av denne typen:

- ✓ Har vi identifisert alle objektene som skal beskyttes?
- ✓ Har vi spesifisert hva de skal beskyttes mot?

Sikring av bærbare maskiner

Selv i IT-alderen gjelder den gamle sannhet om at ingen kjede er sterkere enn det svakeste ledd. Når vi har fått på plass alle våre forsvarsverker, autentiseringssystemer, VPN-forbindelser og så videre, er mobile maskiner som regel vårt svakeste ledd. Vi trenger – og mange organisasjoner har forlenget gjort jobben – en policy for bruk og sikring av organisasjonens *laptops*. Microsoft foreskriver følgende tre punkter i den forbindelse (www.microsoft.com/security/protect):

- Bruk en brannmur
- Hold maskinen oppdatert
- Bruk oppdatert antivirus-programvare

Dette ser enkelt nok ut, men er det motsatte – for alminnelige brukere. Faktum er at vi neppe noen gang kan få god sikring av bærbare maskiner så lenge vi forventer at brukeren skal forstå og ta ansvar for ett eller flere av disse punktene. Selv for eksperter kan dette være krevende nok. For eksempel – hva mener vi med brannmur? Skal den være i maskinen eller utenfor? Hva betyr det å være oppdatert? At vi skal søke etter oppdateringer hver dag? Og så videre.

Her må det annen lut til. Målsettingen er i størst mulig grad å fjerne brukeren fra ligningen. Færre variable gir større enkelhet og bedre sikkerhet. SSL-baserte mekanismer, som vi diskuterer i artikkelen på side 12, er ofte enklest for mobile brukere og hjemmebrukere. De impliserer blant annet fjernkontroll og fjernkonfigurasjon av klienten, uten at brukeren involveres [også enkelte tradisjonelle VPN-produkter har slik funksjonalitet].

Videre er løpende oppdateringer vel og bra, men spørsmålene har lett for å bli flere enn svarene. Vårt råd er å legge vekt på sikringen av nettverket, slik at systemene eksponeres minimalt. En fjernstyrt brannmur på den bærbare maskinen minimaliserer behovet for brukerstyrt oppdateringsprosesser.

Innholds- (virus-) kontroll er viktig på slike systemer, men kan aldri bli bra nok. Derfor er det kritisk at kommunikasjon mellom sentrale systemer og eksterne brukere settes opp slik at smittefaren blir minimal. Vi finner et voksende antall alternativer på markedet i så henseende. Om mulig skal vi unngå dataoverføring fra klienter til sentrale systemer, og alltid sørge for å holde brukerens interaksjoner innenfor rammene av nettleserens SSL-sikrede forbindelser.

Vår *laptop*-policy skal også angi hvem som kan bruke utstyret. Anbefalingen er å være restriktiv: Det er vanskelig å finne argumenter for at andre enn medarbeideren selv skal ha tilgang til virksomhetens verktøy.

Sist, men ikke minst må vår policy bestemme om interne data kan lagres på bærbare systemer. Trenden går klart mot større restriksjoner i så henseende. Dersom lokal lagring tillates, må policy angi hvordan de skal sikres (for eksempel via krypterte filsystemer). Glem ikke å inkludere rutiner for sentral lagring av passord i den forbindelse – i tilfelle brukeren blir 'inkapasitert' og virksomheten trenger innholdet.

- ✓ Har vi evaluert sannsynligheten for at ulike trusler kan materialisere seg?
- ✓ Har vi evaluert de valgte beskyttelsesmekanismene?
- ✓ Har vi evaluert konsekvensene?
- ✓ Står sikringskostnadene i forhold til verdien av objektene som skal sikres?

Spesielt siste punkt viser seg å forårsake overraskelser. For eksempel er det sannsynlig at de valgene vi har gjort med hensyn til beskyttelsesmekanismer vil påvirke måten nettverket overvåkes og styres på. Har vi tatt med konsekvensene av disse forandringene? Forbausende ofte er svaret nei.

Sist, men ikke minst er sikkerhetsarkitekturen et levende dokument som skal løpende justeres i takt med forandringer i virksomheten og infrastrukturen. Blir den liggende urørt i (for eksempel) 12 måneder, er sjansene store for at vi like godt kan begynne på nytt. I mellomtiden har sikkerheten skrantet.

Oppsummering

Mens de aller fleste er enige om viktigheten av å prioritere sikringstiltak og sikkerhetsarbeid, er veien til målet gjenstand for sprikende oppfatninger. Selv i 2003 forekommer det hyppig at sikringstiltak settes i verk uten å være en del av en plan. Det betyr ikke at tiltakene er unyttige, men i de aller fleste tilfeller blir veien til reell IT-sikkerhet lenger og mer kostbar på denne måten. Med et veldefinert mål og en plan, maksimaliserer vi sjansene for riktige resultater i forhold til behovene.

Om trusler og mekanismer forandrer seg kontinuerlig, er mange av metodene som leder frem til en god sikkerhetsarkitektur de samme i år etter år. For praktiske råd og metodebeskrivelser, henviser vi til artikkelserien i Mellvik-Rapporten nr. 34-44. Disse utgavene er tilgjengelige i pdf-format via Web-tjenesten, se side 35.

Et sikkert ståsted

I neste utgave presenterer vi en samling statistiske data og tilhørende observasjoner knyttet til utviklingen på sikkerhetsfronten. Videre diskuterer vi ideer og tanker som er grunnleggende for etablering av god sikkerhet og for forståelse av selve problematikken. Som så ofte er tilfelle, bruker vi gjerne mer tid på detaljene enn på helheten. Konsekvensen i forbindelse med sikkerhet og sikring er at stor innsats gir beskjedne resultater.

Flere tips om policy

Policy – ikke bare knyttet til sikkerhet, men til bruk av verktøy i sin alminnelighet – hører til de hyppigst forekommende temaer i våre diskusjoner med fagpersoner og IT-ledere i inn- og utland. Derfor fortsetter vi rekken av praktiske hint og gode råd i neste utgave, og fyller dessuten på med en artikkel om lagrings-policy (se baksiden for detaljer).