Internrevisjon av cyber security

– hvordan benytte angrepssimulering for å avdekke de reelle risikoene

Av
MAGNUS FELDE
Magnus er manager i Deloitte Cyber Risk Services hvor han leder fagområdet strategi og risikostyring. Han har en mastergrad innen informasjonssikkerhet samt en Master of Management fra BI, og har lang erfaring med gjennomføring av risikovurderinger og revisjoner på tvers av ulike sektorer.

Av
LINN KRISTIN KLAUSEN
Linn er konsulent i Deloitte Cyber Risk Services, og har en master i etterretning og internasjonal sikkerhet fra King's College London. Hun arbeider med trusseletterretning og informasjonssikkerhet.

Innovasjon, informasjonsdeling og tillit er tre fundamentale vekstdrivere for virksomheter i dagens digitale samfunn. Digitalisering introduserer forretningsmuligheter gjennom fremvekst av nye virksomheter, endring av eksisterende virksomheter, nye produkter og tjenester. Begrepet cyber kan oversettes på norsk til det digitale rom. Økt digitalisering introduserer nye risikoer som må identifiseres og håndteres.

Mange nye virksomheter baserer sin forretningsidé på omfattende innsamling og analyse av data, ofte i samarbeid med tredjepartsaktører. Disse er spesielt utsatt for lekkasjer eller misbruk av informasjon. Facebook-skandalen er et nylig eksempel på dette. Slike hendelser vil medføre tap av tillit og kunne trigge behov for økt regulering. Digitalisering medfører en større forretningsmessig avhengighet av IT-løsninger. Nedetid vil kunne medføre store forretningsmessige- og økonomiske konsekvenser. Banker og telekom-virksomheter har erfart viktigheten av å sørge for oppetid av systemer.

Enkelthendelser, være seg tilsiktede eller utilsiktede, vil kunne resultere i store negative konsekvenser for virksomheter. Eksemplene på slike saker er mange. Mærsk har rapportert et tap på 300 millioner dollar som følge av at deres IT-systemer ble utilgjengelige etter å ha blitt utsatt for et løsepengevirus kalt «NotPetya» [1]. Facebook er i hardt vær som følge av at informasjon om 85 millioner av deres brukere ble delt med Cambridge Analytica, som igjen har brukt informasjonen til analyser. Disse er solgt til klienter. Hva de endelige konsekvensene av saken vil innebære for Facebook gjenstår å se, men etter at nyheten ble kjent har markedsverdien av virksomheten blitt redusert med 100 milliarder dollar [2].

En viktig premiss for enhver revisjon vil være å avdekke hvorvidt hensiktsmessige tiltak er implementert i tråd med etablert risikoappetitt, og hvorvidt tiltakene fungerer som tiltenkt. Den økte cyber risikoen knyttet til digitalisering fordrer at internrevisjonen vurderer virksomhetsstyring og kontroll av sikkerheten i det digitale rom. Spørsmålet er hvordan man best bør gå frem for å avdekke dette.

Et komplekst digitalt økosystem bestående av en rekke aktører kombinert med høy endringstakt tilsier at det vil være utfordrende for enkeltpersoner å vurdere den faktiske sikkerhetstilstanden i organisasjonen. Deloitte benytter et spesialtilpasset rammeverk for dette. I tillegg gjennomfører vi angrepssimulering med hjelp av et teknisk ekspertteam kalt «red team» for å avdekke sikkerhetshull. Vår erfaring er at denne kombinasjonen av aktiviteter gir et svært godt bilde av dagens situasjon i virksomheten, og danner et godt grunnlag for å definere en tiltaksplan som er med på å redusere den reelle risikoen.

Trusselbildet i det digitale rom er i stadig endring, og kompleksiteten tilsier at man må håndtere cyber-sikkerhet nyansert og dynamisk. Trusselnivået og risikoeksponeringen må forstås opp mot spesifikke komponenter som inngår i et helhetlig styringssystem for cyber sikkerhet – og bør være integrert i den totale virksomhetsstyringen. I utarbeidelse av styringssystem er det viktig å forstå trusselbildet, og se dette opp imot hvilke kapabiliteter som er nødvendig å ha på plass for å sikre informasjonsverdier hensiktsmessig. Disse komponentene kan deles inn på ulike måter, og det finnes en rekke rammeverk og god praksis som beskriver slike komponenter.

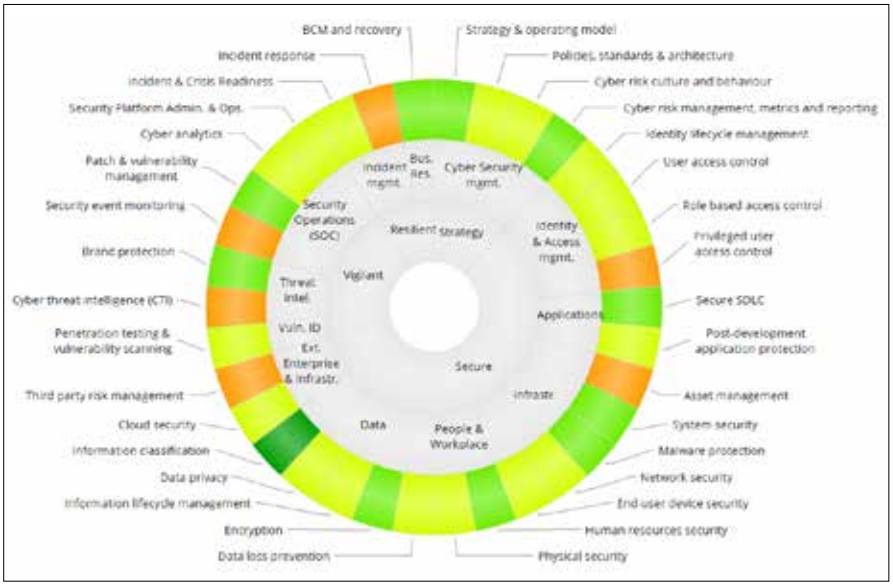
Deloittes rammeverk, kalt *Cyber Strategy Framework (CSF)* inneholder god praksis ift. cyber-kontroller knyttet opp mot risiko og type virksomhet. Et dedikert team sørger for å oppdatere dette i tråd med utviklingen av cyber-risiko og vår erfaring. Rammeverket muliggjør en strukturert og risikobasert tilnærming for å vurdere cyber tilstanden i virksomheten,

og med utgangspunkt i dette utarbeide handlingsplaner. Rammeverket hjelper oss med å identifisere verdier, trusselaktører og manglende eller mangelfulle kontroller.

Innen cyber-sikkerhet eksisterer det en rekke ulike standarder og rammeverk som benyttes for å etablere hensiktsmessige sikkerhetstiltak, og det er viktig å bruke et metodeverk som er dekkende og tilpasset den aktuelle virksomheten. International Organization for Standardization (ISO) 27001/2, Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), og Information Security Forum (ISF) Standard of Good Practice for Information Security er alle eksempler på rammeverk som benyttes for å ivareta cyber-sikkerhet.

Uavhengig av hvilken standard eller rammeverk som er benyttet for å håndtere cyber-sikkerhet kan CSF benyttes for å utføre en vurdering av etablerte tiltak. CSF kan benyttes selvstendig eller som en kartlegging mellom andre rammeverk. Videre vil resultatene fra CSF-vurderingen automatisk kunne presenteres opp mot ISO 27002, NIST Cybersecurity framework og CIS Top 20 Controls.

Center for Internet Security (CIS) er en ikke-for-profitt organisasjon som regelmessig utarbeider 20 sikkerhetskontroller for cyber, i prioritert rekkefølge. Ved å implementere kun de fem første kontrollene estimeres det at cyber-risikoen kan reduseres med omtrent 85%. CSF er bygd opp på tilsvarende måte, og oppdateres jevnlig for å være aktuell opp mot det gjeldende trusselbildet og god praksis. Hvert område innen cyber rangeres på en modenhetsskala fra 1-5, der etablering av de grunnleggende kontrollene på nivå 1-3 vil redusere brorparten av risikoen. Grunnet stadig mer sofistikerte angrep og flere digitaliserte løsninger, ser



CSF-hjulet.

vi likevel at området i stor grad er hendelsesdrevet. Risikostyring på området blir dermed ofte vilkårlig. I mange tilfeller er avanserte kontroller på plass mens det helt grunnleggende mangler. For å vite hvilke komponenter som burde være på plass anbefaler vi en risiko-basert tilnærming til cyber-sikkerhet, med forståelse for forretningskontekst og trusselbilde.

Deloitte deler opp en cyber-modenhetsvurdering i fem faser som vist under.

I den innledende fasen kartlegges forretningskonteksten og bedriftens viktigste informasjonsverdier (kalt bedriftens «kronjuveler»).

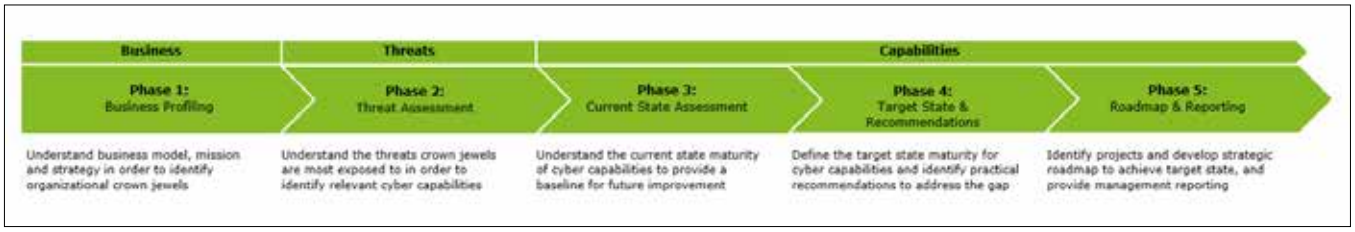
Fase 1 blir et naturlig bakteppe til fase to, hvor en trusselvurdering utarbeides. Det er viktig å identifisere aktuelle trusselaktører, deres taktikker, teknikker og prosedyrer, samt sannsynlige angrepsvektorer og trusselscenarioer. Disse utarbeides basert på tidligere angrep på bedrifter med linkende profil og eksponering.

Fase tre er en analyse av virksomhetens modenhet, med de to foregående fasene (forretningsprofilering og trusselvurdering). Denne fasen er en gjennomgang av virksomhetens nåværende modenhet. Dette kan gjøres på flere forskjellige måter. Cyber sikkerhet deles opp i 34 kapabiliteter som i kombinasjon vurderer tiltak for å forhindre, oppdage og respondere på sikkerhetshendelser.

Disse områdene blir gradert på en modenhetsskala fra 1-5, fra ad-hoc og varierende praksis til systematisert og optimalisert styring med kontinuerlig forbedring gjennom både inkrementelle og innovative endringer.

For å fastsette modenheten kan flere forskjellige metoder benyttes.

1) Vi gjør en dokumentgjennomgang og gjennomfører intervjuer innenfor de ulike kapabilitetene med nøkkelansatte i linjeorganisasjonen. De kan ofte hjelpe til med å identifisere svakheter i styringen, som kan ha mange forskjellige årsaker. Disse svakhetene rangeres. Resultatet sammenliknes med tilsva-



Cyber modenhetsvurderingens fem faser.

rende bedrifter; i samme industri, fagområde, av tilsvarende størrelse og trusselprofil. Dette gjøres via et stort datagrunnlag – all informasjonen vi henter inn anonymiseres og aggregeres for sammenlikning og kalibrering – og er nyttig for virksomhetene da det viser hva som er beste praksis i markedet i dag innenfor cybersikkerhet.

2) Deloitte tar ofte stikkprøver for å teste kontrollene som er implementert. Slike tester er viktig, og viser effekten av implementerte tiltak. De gir imidlertid ikke svar på om en hacker kan omgå tiltaket.

3) For å avdekke hull i sikkerhetsarkitekturen til virksomheten utfører Deloitte en angrepssimulering med et ekspert team kalt «red team». Med utgangspunkt i informasjonen vi identifiserer i de to første fasene vil vi kunne definere scenarioer og mål som angrepssimuleringen skal forsøke å oppnås. Dette vil typisk være scenarioer som vil få store konsekvenser for virksomheten dersom en angriper lykkes. Dette kan være å teste om vi kan overføre en betydelig pengesum fra en finansinstitusjon eller stoppe trafikken hos en infrastrukturoperatør ved å tilegne oss tilgang til kjernesystemene i virksomheten.

Angrepssimuleringen blir skreddersydd til den enkelte virksomhet, og i likhet med reelle angrep blir «minste motstands vei» utnyttet for å oppnå sluttmålet. Her vil inngangsporten kunne være å fysisk lure seg inn, utnytte eksternt eksponerte IT systemer eller sende såkalt «spear phishing» e-poster til ansatte. Angriperen vil bruke ervervede tilganger for å komme seg videre inn i organisasjonens infrastruktur på jakt etter hovedmålet. Nettopp fordi målet er å oppnå adgang til kjernesystemene er det viktig at angrepsteamet har en tett dialog med nøkkelpersonene i virksomheten for å sikre en god og trygg prosess.

Ettersom det ikke vil være mulig å forhindre ethvert angrep vil det også være viktig å ha kapabiliteter til å oppdage og respondere på hendelser som inntreffer. Som en del av angrepssimuleringen er det derfor som regel ønskelig å teste organisasjonens evne til å oppdage slike angrep. Dette fordrer at kun noen utvalgte nøkkelpersoner er gjort kjent med testen på forhånd slik at testen blir så realistisk som mulig. I etterkant av testen vil det være mulig å raskt identifisere hvor angrepet burde ha vært oppdaget slik at etablerte tiltak kan forbedres, samt identifisere områder som krever økt overvåking.

Resultatene fra en slik test gir således svært håndfaste observasjoner som kan brukes for å definere anbefalte tiltak. Resultatene fra testene vil videre være svært virkningsfulle ved at man har bevist at et konkret scenario faktisk er mulig, og ikke bare «sannsynlig». Dette er svært nyttig for å gi helt konkrete anbefalinger til forbedringer av sikkerhetsarkitekturen.

Fase 1-3 legger grunnlaget for en handlingsplan som fastsettes i fase 4, og et transformasjonsprogram som fastsettes i fase 5.

I fase 4 vurderes det om eksisterende sikkerhetstiltak er hensiktsmessige. Dersom vi i fase 3 avdekket manglende eller lite effektive tiltak vil vi etablere en handlingsplan som definerer hvilke tiltak virksomheten på kort og lang sikt bør etablere for å operere innenfor en akseptabel risiko. Det er viktig at denne fasen utføres i tett samarbeid med virksomheten, og at det vurderes hvordan anbefalingene passer opp mot forretningskontekst og øvrige handlingsplaner.

Fase 5 – transformasjonsfasen - er typisk et omfattende omstillingsprosjekt og dekker som regel alle de 34 kapabilitetene som er identifisert innenfor cyber-sikkerhet. Denne fasen utføres derimot ikke i tradisjonelle internrevisoroppdrag, og omtales derfor ikke videre i denne artikkelen.

De iboende cyber-risikoene som økt digitalisering medfører må som nevnt identifiseres og håndteres. Rammeverket som er beskrevet i denne artikkelen hjelper organisasjoner med å avdekke hvorvidt hensiktsmessige tiltak er implementert og om disse fungerer som tiltenkt – for således å kunne vurdere om risikoen ligger på et akseptabelt nivå.

Grunnet stor endringstakt, et dynamisk trusselbilde og stadig nye sårbarheter som kan utnyttes, er det viktig å jevnlig vurdere om man har de riktige tiltakene på plass. Rammeverket med tilhørende verktøy gir mulighet for enkelt å foreta en ny evaluering for å se utviklingen av pågående arbeid eller avdekke hvorvidt nye tiltak er nødvendig. Dette vil bidra til å styrke styring og kontroll av risikoene i det digitale rom (cyber risikoer).

Modenhet	Beskrivelse
1	Grunnleggende: kapabilitetene er udokumenterte og i konstant forandring (ad-hoc)
2	Gjentagende: repeterende kontroller, men ikke fullt dokumenterte eller dekkende for området – det er fortsatt noe grunnleggende.
3	Definert: definert styringssystem, formell dokumentasjon, fastsatt scope og eierskap til prosesser, rutiner eller systemer. Styringen er gjeldende på tvers av bedriften.
4	Styrt: tilsier aktiv styring der ytelse måles regelmessig og tiltak identifiseres.
5	Optimalisert: kapabiliteten er under kontinuerlig forbedring gjennom både inkrementelle og innovative endringer. Det er avanserte og industri-ledende implementering med full dekning.

[1] https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff
[2] http://fortune.com/2018/03/26/facebook-stock-ftc-investigation-cambridge-analytica/