Kontakt oss

For mer informasjon om vår scenariobaserte analyse, ta kontakt med en av våre konsulenter.

Hans Christian Pretorius
KPMG Advisory, Cybersikkerhet
T: +47 908 79 077
E: hans.christian.pretorius@kpmg.no

Andreas Orset
KPMG Advisory, Cybersikkerhet
T: +47 938 29 158
E: andreas.orset@kpmg.no

kpmg.no/cybersikkerhet

Vår metodikk

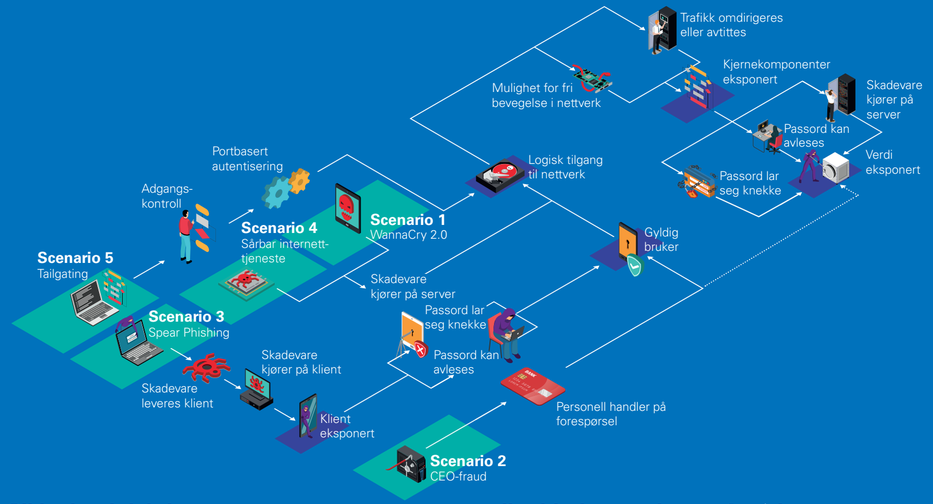
KPMG har meget god kunnskap om hvordan trusselaktører opererer. 90 % av cyberangrep bruker e-post som angrepsvektor, og i 10 % av tilfellene benyttes svakheter i internettbaserte tjenester. Basert på denne kunnskapen tar KPMG utgangspunkt i et "angrepsflytskjema". Dette skjemaet mapper vi mot de sikkerhetsmekanismene som må være på plass for å hindre et vellykket datainnbrudd. Basert på det aktuelle scenarioet henter vi ut de ISO-kontrollene som må være på plass for å hindre trusselaktøren fra å kunne gjennomføre et vellykket cyberangrep på virksomheten.

For hvert scenario gjør vi en vurdering av hvor viktig hver kontroll er for å stoppe trusselaktøren. Hvorvidt kontrollen er hensiktsmessig utformet og etterlevd blir så vurdert, før vi vurderer om den er tilstrekkelig god for å hindre trusselaktøren fra å nå verdiene. Hver relevante kontroll blir vurdert, og til slutt trekker vi en samlet konklusjon for hvert scenario ved hjelp av standardiserte sannsynlighetsord.

Analysens datagrunnlag hentes inn gjennom spørreskjema og intervjuer med ansatte i virksomheten.

Hva lykkes angriperen med?

Angriperen går systematisk til verks for å oppnå tilgang til virksomhetens verdier. Basert på kunnskap om angriperens metodikk har vi utarbeidet et angrepsflytskjema som inkluderer våre fem scenarioer.



Sikkerhet i dybden …

Prinsippet om sikkerhet i dybden har blitt et etablert prinsipp i sikkerhetsmiljøet. Flere nivåer av tiltak hindrer eller begrenser angriperes evne til å skade systemer. Å vektlegge alle nivåer av sikkerhet i like stor grad er ikke nødvendigvis hensiktsmessig eller kostnadseffektivt. Kunnskap om de ulike nivåene av cybersikkerhet og virksomhetens modenhet i de ulike nivåene bør være sentralt i virksomhetens beslutningsprosesser.

… eller hindre angriperen fra å komme seg videre

Kunnskap om angriperens fremgangsmåte bør ligge til grunn for ressursprioriteringer tilknyttet cybersikkerhet. Nødvendigheten av kostbare sikkerhetstiltak i dybden blir mindre dersom man iverksetter tilstrekkelige sikringstiltak som hindrer angriperen i tidlige faser.

Klar for cyber-angrepet?

Scenariobasert risikoanalyse – med dagens trusselbilde i fokus

kpmg.no/cybersikkerhet

Dagens trusselbilde

Norske bedrifter digitaliserer stadig flere arbeidsprosesser, tjenester og funksjoner. Ettersom verden blir mer og mer digital, blir truslene også i økende grad digitale. Privatpersoner, virksomheter og nasjoner står overfor en økende grad av risikoer tilknyttet det digitale domenet. Kriminelle enkeltpersoner og grupperinger benytter cyberangrep for å tilegne seg finansielle verdier, terrorceller for å skape frykt, og statlige aktører til etterretning eller som del av en angrepsstrategi. Utfordringene i det digitale rom er grenseoverskridende – på tvers av land, sektorer og virksomheter.

I norsk næringsliv kan alle kan bli offer for økonomisk kriminalitet og destruktiv skadevare, eller bli indirekte skadet som følge av målrettede angrep mot enkelte virksomheter og bransjer.

Kriminelle aktører svindler norske virksomheter for millionbeløp på nett, og sofistikerte digitale angrepsverktøy er viktige drivkrefter bak globale løsepengekampanjer og stadig mer omfangsrike tjenestenektangrep. Målvalg og observert angrepsmetodikk knytter også mye av aktiviteten i cyberdomenet til hemmelige tjenester med store ressurser til nettverksoperasjoner og utvikling av skadevare. De vanligste metodene for infiltrasjon er ved bruk av målrettede e-poster med vedlegg eller lenker, planting av skadevare via kompromitterte nettsider eller direkte utnyttelse av tekniske sårbarheter.

I dagens trusselbilde er politiske, militære og økonomiske mål samt virksomheter innen forsvarsindustri, høyteknologi og kritisk infrastruktur særlig utsatt. Samtidig treffer målrettede og ikke-målrettede digitale angrep bredere enn tiltenkt. De som ikke har beskyttet seg må forvente å bli rammet.

Scenariobasert risikoanalyse

En cybersikkerhetsanalyse som tar høyde for dagens trusler

WannaCry 2.0

Våren 2017 ble verden rammet av løsepengeviruset WannaCry. Cyberangrepet førte til at innholdet på mer enn 200 000 enheter i 150 land ble kryptert, og viktige datasystemer mistet sin tilgjengelighet. Angrepet kostet ofrene flere milliarder dollar og viste hvor skadelige løsepengevirus potensielt kan være.

Et nytt WannaCry kan inntreffe, og utnytte nye sårbarheter i klient. Vil din virksomhet kunne stå imot WannaCry 2.0?

MULIGE KONSEKVENSER:
- TAP AV DATA
- OMDØMMETAP
- NEDETID
- SKADE PÅ TEKNISK UTSTYR

CEO-fraud

Direktørsvindel, eller CEO-fraud, er sosial manipulering som har til hensikt å lure en økonomiarbeider til å betale en faktura eller overføre penger til en konto. Svindleren utgir seg for å være en person i ledelsen i virksomheten, og svindelen utføres ofte ved bruk av e-post eller SMS.

Svindlerne blir stadig mer utspekulerte i sine fremgangsmåter, og gjør grundig forarbeid før de gjennomfører cyberangrepet.

MULIGE KONSEKVENSER:
- OMDØMMETAP
- FINANSIELLE TAP

Spear Phishing

Spear Phishing er en form for nettfiske der trusselaktøren sender en e-post til en spesifikk organisasjon eller person, med det formål å oppnå tilgang til sensitiv informasjon. E-posten inneholder enten et vedlegg med skadevare eller en lenke som tar offeret til et nettsted med skadevare.

I likhet med CEO-fraud utgir trusselaktøren seg for å være en tillitvekkende person, gjerne fra en velkjent organisasjon.

MULIGE KONSEKVENSER:
- TAP AV DATA
- OMDØMMETAP
- NEDETID
- SKADE PÅ TEKNISK UTSTYR

Sårbar internett-tjeneste

Trusselaktører søker etter sårbarheter i applikasjoner, systemer og nettverk for å oppnå logisk tilgang til nettverk. Feil i konfigurasjon eller manglende patching kan utnyttes i målrettede angrep.

I noen av de største cyberhendelsene i Norge den siste tiden har trusselaktørene utnyttet sårbare internettjenester.

MULIGE KONSEKVENSER:
- TAP AV DATA
- OMDØMMETAP
- NEDETID
- SKADE PÅ TEKNISK UTSTYR

Tailgating

Tailgatinger en form for sosial manipulasjon som innebærer at en trusselaktør tar seg inn i et adgangsbegrenset område ved å følge etter en person med tilgang til området. Den ansatte kan enten slippe inn trusselaktøren med overlegg eller det kan være en uaktsom handling.

Ved hjelp av tailgating kan trusselaktøren få tilgang til eiendeler og data, samt tilgang til virksomhetens nettverk.

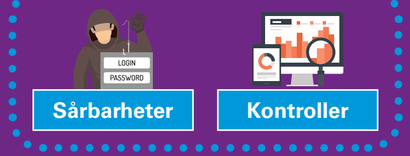
MULIGE KONSEKVENSER:
- TAP AV DATA
- OMDØMMETAP
- SKADE PÅ SYSTEMER
- SKADE PÅ TEKNISK UTSTYR

Kan din bedrift stå imot angrepet?

I møte med dagens digitale trusler er det viktig å ha god kontroll over egen cybersikkerhet.

Gjennom en analyse av selskapets sårbarheter og kontrollmekanismer vurderer vi hvorvidt selskapet er i stand til å stå i mot trusselaktører som benytter kjent angrepsmetodikk.

Analysen resulterer i en scenariorapport som stadfester selskapets modenhet og evne til å stå imot angrepet.



Individuell vurdering

Basert på scenarioet og utvalgte ISO 27002-kontroller

Sannsynligheten for at din bedrift kan stå imot angrepet