Cyber/informasjonssikkerhetsområdet, sikkerhetstesting som en del av internrevisjonen

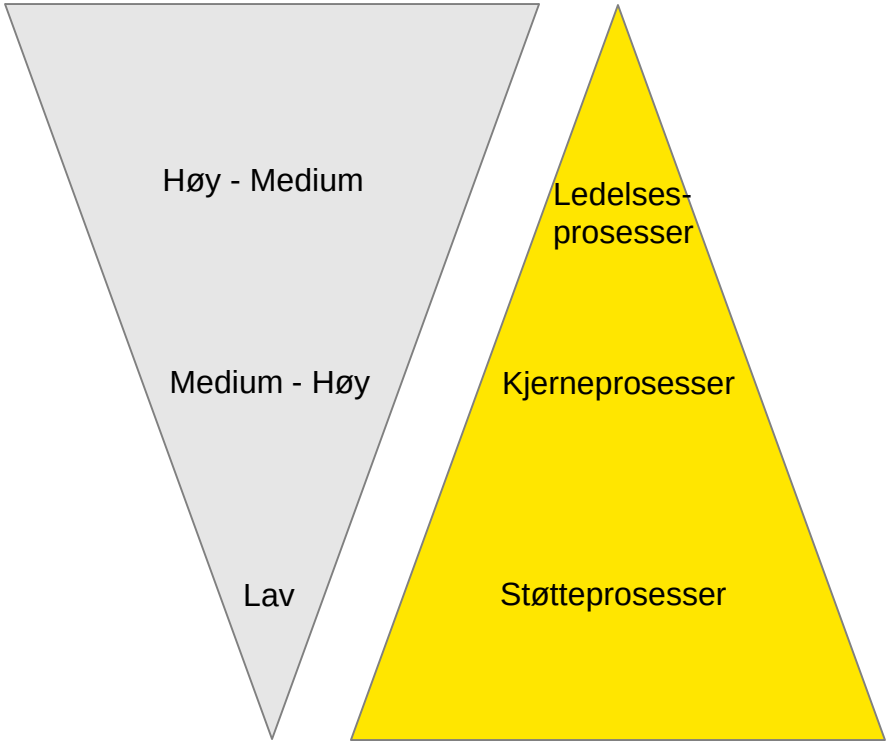
Aina Karlsen Røed

The better the question. The better the answer.
The better the world works.

Building a better working world

Internrevisjonen bør innrettes slik at den bruker ressursene hensiktsmessig og effektivt der det er størst risiko

For at internrevisjonen skal tilføre merverdi og bidra til forbedringer må den ha riktig fokus og bruke ressursene hensiktsmessig og effektivt - størst fokus på kjerne- og ledelsesprosesser som representerer størst risiko og vesentlighet for virksomheten og dens samfunnsoppdrag



Eksempler på fokusområder:

- Virksomhets- og risikostyring
- Strategi
- Forbedrings- og endringsprogrammer
- Tilskuddsforvaltning
- Saksbehandling
- Myndighetsutøvelse
- Beredskap
- Finansieringsmodeller
- Etikk og samfunnsansvar
- HR og kompetanseutvikling
- IT og digitalisering
- **Cyber og informasjonssikkerhet**
- Anskaffelser
- Økonomistyring

Informasjonssikkerhetsundersøkelse viser

EY Global Information Security Survey 2017-2018 (GISS)
Svarene hentet ut for alle deltakere fra offentlig sektor globalt.
Norske og Nordiske deltakere i undersøkelsen.

71%

Har økt cybersikkerhets-budsjettet det siste året. Av disse hadde 35% en økning mellom 5-15%. Samtidig mener 55% at det er nødvendig å øke finansieringen med opp til 25%.

72%

Vil se en videre økning i budsjettet for cybersikkerhet det neste året, men bare 16% forventer en økning på mer enn 25%.

4%

Sier at informasjonssikkerhets-funksjonen fullt ut tilfredsstiller organisatoriske behov.

Deteksjon av hendelser regnes som den mest sannsynlige faktoren til budsjettøkning i løpet av det neste året.

De mest anerkjente sårbarheter og trusler er skadelig programvare (malware), phishing og uforsiktige eller uvitende ansatte.

Topp tre sannsynlige angrepskilder er: Uforsiktig arbeidstaker (74%), organiserte kriminelle (55%) og uorganiserte hackere (53%)

25% har ikke et definert program for sårbarhets-identifisering mens bare 9% har ikke et databeskyttelses-program.

57% har hatt en nylig, betydelig cybersikkerhets-hendelse. 13 % ble oppdaget av en SOC, mens 32% av intern virksomhetsfunksjon.

Hovedprioritetene for de neste 12 månedene er sikkerhetsbevissthet og opplæring (63%), og forebygging av datatap (61%)

22% har en formell prosess for detektering av hendelser
.

50% anser det som «usannsynlig» eller «svært usannsynlig» at organisasjonen vil oppdage et sofistikert cyberangrep.

Penetrasjonstesting og overvåking av nettverkssikkerhet er de SOC-funksjonene som er mest utkontraktert. 29% har ikke en SOC.

65% sier at styret ikke har nok kunnskap om informasjonssikkerhet.

…samtidig blir truslene mer og mer sofistikerte

Uerfaren angriper
(Script Kiddies)
Nivå 1

Erfaren angriper
(Hacker)
Nivå 2

Industrispionasje
(Insider)
Nivå 3

Statlig sponset angrep
Advanced Persistent Threat, Hacktivism, ID tyveri
Nivå 4

Eksperimentering
- Du blir angrepet fordi du er på internett og det eksisterer mange sårbarheter

Tjene penger
- Du er under angrep fordi du er på internett, og en angriper mener du har informasjon verdt å stjele

Inside-jobb
- Din nåværende eller tidligere ansatt forventer økonomiske fordeler for sin intellektuelle eiendom

Målrettet angrep
- Du blir angrepet på bakgrunn av hvem du er, hva du gjør eller verdien av immaterielle rettigheter
- Cyberangrep benyttes for å nå politiske eller økonomiske mål
- Økende tyveri av personlig identifiserbar informasjon (PII)

1980s/1990s ····· 2018

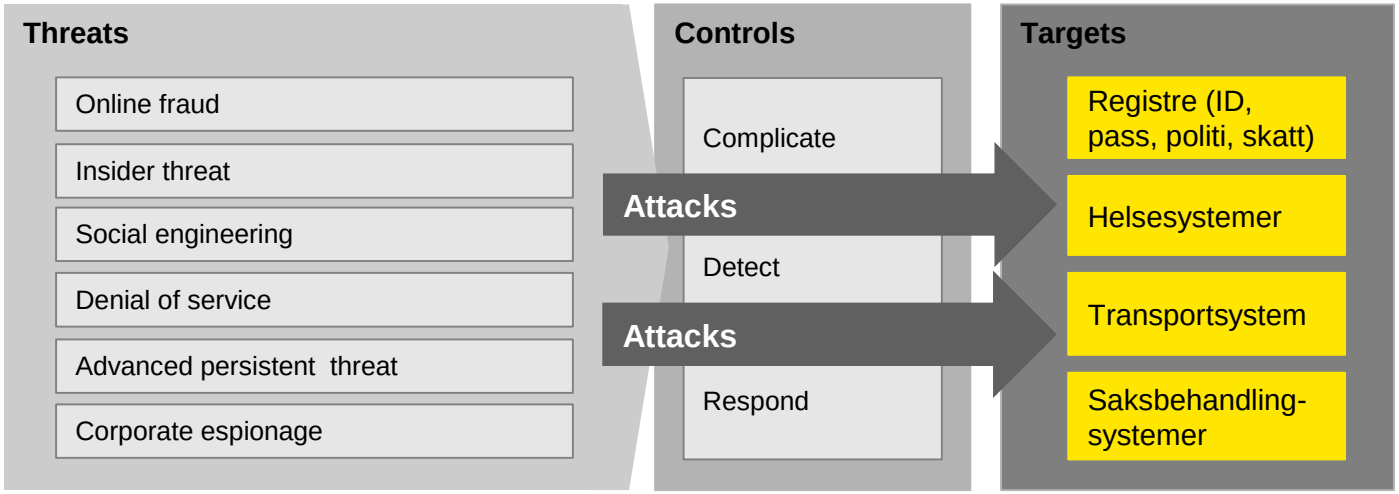
Hva er en sikkerhetstest?

Enkel sikkerhetstest

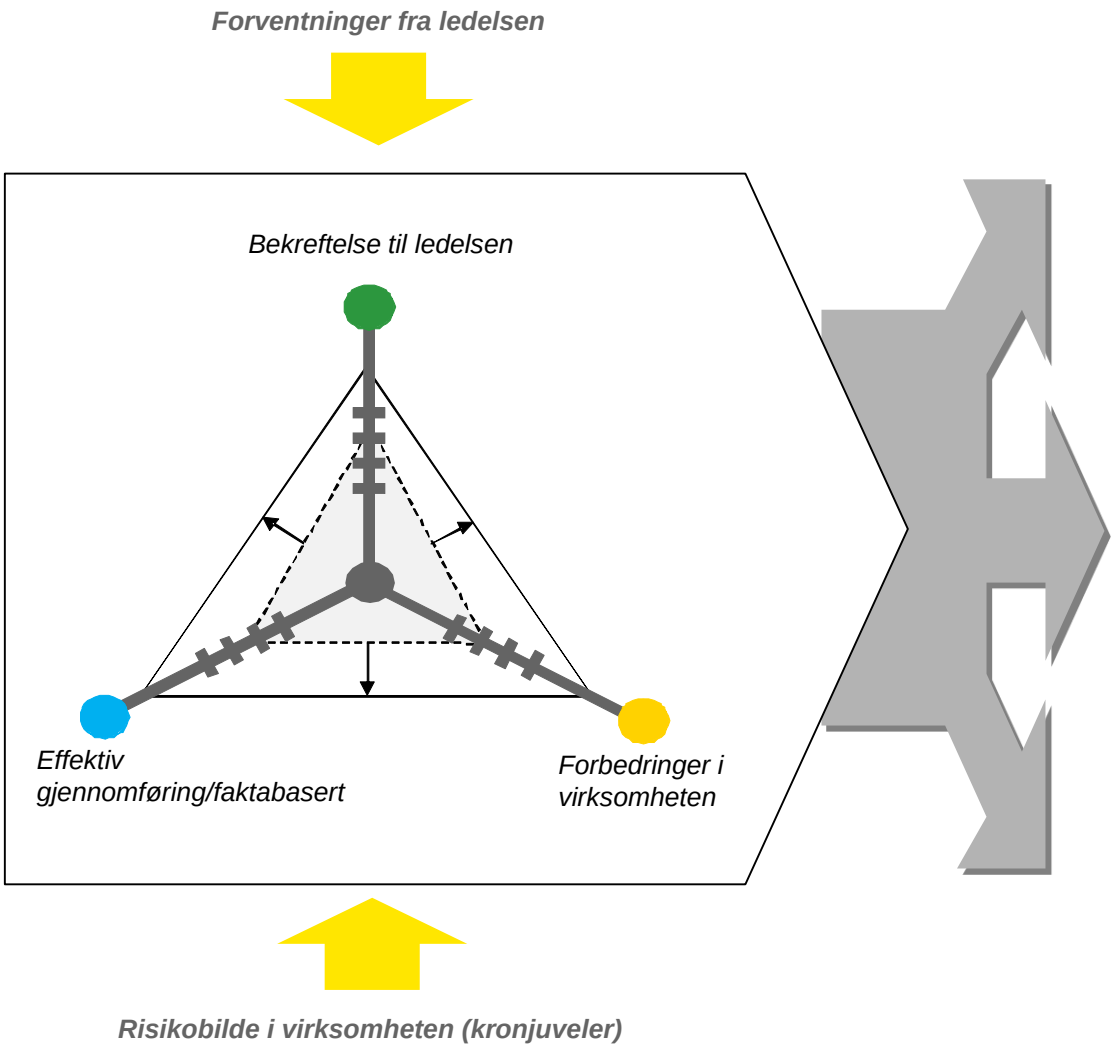
- En sikkerhetstest er en effektiv måte å teste hvor effektive og godt implementert tekniske kontrollene er i systemer, infrastruktur, databaser etc.
- Gjennom en test vil vi oppdage og eventuelt utnytte identifiserte svakheter for å avgjøre grad av risiko knyttet til sårbarheten.
- Vi vil bruke testmodeller og scenarioer som etterligner hvordan dette kunne skjedd dersom noen faktisk hadde brutt seg inn i virksomhetens systemer

Hva sitter dere igjen med?

- Gjennom å utføre sikkerhetstester (periodisk) reduserer man risiko for at angripere får tilgang til eller kontroll over virksomhetens systemer.
- Ved at vi bruker de samme metoder og teknikker som et faktisk angrep i sikkerhetstesten vil virksomheten få et reelt bilde av faktisk risiko.



Hvorfor gjøre sikkerhetstesting som en del av internrevisjonen?



Strategisk og verdiskapende rådgiver
Internrevisjonen fungerer som en katalysator på strategiske initiativer, utfordringer og endringer i organisasjonen.
Sikkerhetstestingen vil derfor både hjelpe ledelsen å bedre forstå de forretningsmessige konsekvensene av sårbarhetene samt at resultatene av testingen vil både måtte kommunisere til teknisk og ikke-tekniske personer noe som ofte i dag ikke er tilfelle med en rekke av testene som utføres i utviklingsløp eller ad-hoc av IKT-miljøene selv

Virksomhetsinnsikt
Internrevisjonsfunksjonen er designet for å gi høy kvalitet og relevant virksomhetsinnsikt, som en integrert del av sine aktiviteter.
Sikkerhetstesting som en del av internrevisjon er derfor en stor fordel da man har god innsikt om virksomheten og dermed potensielt også hvor risikoen er høy og hvor de viktigste informasjonsverdien ligger. Man kan dermed bidra til å sette fokus på og bidra til prioritering av forbedringer på sikkerhet der det «monner» mest.

Kontroll og etterlevelse
Internrevisjonen er fokusert på å vurdere design og effektiviteten i internkontrollen på de områdene som er skissert i mandatet.
Sikkerhetstesting er således et meget effektivt verktøy for å teste internkontrollen på sikkerhetsområdet. Det gir gode faktabaserte bevis som er vanskelig å argumentere imot.

Våre kapasiteter - Nordic Security Center team i Oslo

Tekniske cyber-ressurser

- Våre nordiske tekniske kapasiteter og det nordiske sikkerhetssenteret (NSC)
- Operasjonsrom i Oslo
- 15 dedikerte tekniske sikkerhetskonsulenter
- Våre ressurser har blant annet CISSP, OSCP, GPEN, CEH, CPT, GWAPT, GSOC, GCWN, GCFA, CREA, ISO 27001 Lead Implementer, CISA, ITIL Foundations v3, PRINCE2 Foundation sertifiseringer
- Doktorgrad i sikkerhetsbevissthet og kryptologi
- Mange av ressursene er sikkerhetsklarerte
- EY har en sikkerhetsavtale med forsvaret og leverandørklarering. Vi kan oppbevare informasjon tom. BEGRENSET

Vi gjør årlig en rekke sikkerhetstester som en del av vår rolle som internrevisor eller som støtte til internrevisjoner i offentlig og privat sektor

Nordic Security Center (NSC)

- NSC er et ISO27001 sertifisert sikkerhetssenter, og alle medlemmer av senteret er aktivt involvert i å både opprettholde og etterleve de krav som blir satt av denne standarden på daglig basis. Alle medlemmer av det nordiske sikkerhetssenteret er jevnlig involvert i trening og opplæring for å sikre at ferdigheter og kunnskap innen informasjonssikkerhet er oppdaterte og relevante.
- NSC hjelper våre kunder med håndteringen av komplekse tekniske vurderinger og utføring av kvalitetssikringsprosjekter som en del av større bedriftsinitiativer som digitale transformasjoner, restruktureringer, utsetting og nyutvikling av elektroniske tjenester, internrevisjon m.m

EY Nordic Security Center (NSC)

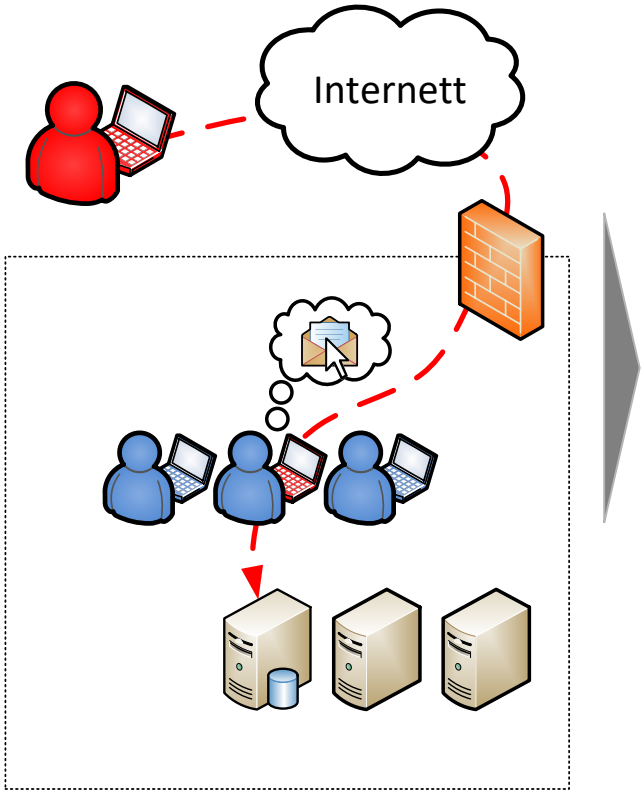
NORSK AKKREDITERING MSYS 001

ISO27001 Certified Information Security ManagementSystem

Case – sikkerhetstest

Angrepsvinkel, omfang og avgrensninger (et eksempel)

Phishing er en svært populær angrepsvektor blant angripere som ønsker å omgå beskyttelsesmekanismer i nettverk og skaffe seg et fotfeste internt i en virksomhet. Når fotfeste er oppnådd på den ansattes datamaskin kan angriperen utforske det interne nettverket på jakt etter sensitiv informasjon, eller gjennomføre andre uønskede handlinger (f.eks. introdusere kryptovirus). Internrevisjonen søker å kartlegge motstandsdyktighet mot slike scenarioer.



Risiko og revisjonsmessig angrepsvinkel

Forslaget er å utføre en sikkerhetstest basert på to testaktiviteter:

1. **Phishing** gjennomføres så nært som mulig opp mot en angripers metode.

   E-postutsendelse til utvalgte ansatte for å så kartlegge hvor mange som klikker på lenken.

   Analysere virksomhetens motstandsdyktighet mot Phishing og ondsinnet kode som sendes per epost – forsøke å etablere lokal tilgang på brukerens PC

2. **Intern sikkerhetstest** utføres ved å benytte opparbeidet lokal tilgang gjennom Phishing for å se hva en angriper kunne kompromittert fra dette ståstedet

   Manuell rekognosering og bruk av veiledede, automatiske skanne-verktøy for å kartlegge potensielle svakheter i det interne datanettverket.

Forutsetninger og avgrensninger

- Revisjonen vil ikke utføre skadelige phishing-momenter, samt at det etterstrebes å anonymisere eventuelle kompromitterte brukere.
- Revisjonen vil i sikkerhetstesten ikke dekke IP-adresser utover det som blir skriftlig avtalt.

Eksempelscenario og typiske aktiviteter

Eksempler på angrep som kan utprøves i et slikt prosjekt er for eksempel:

- Tilegne seg rettigheter på maskinen utover det som er ment for ansatte
- Installasjon og distribusjon av skadelig programvare og omgåelse av antivirus og andre beskyttelsesmekanismer
- Uautorisert tilgang til bedriftssensitiv informasjon, kritiske systemer og databaser
- Evaluering av virksomhetens evne til å detektere og respondere på et slikt angrep

Hva kan en angriper utrette av skade på kort tid gjennom en ansattmaskin?

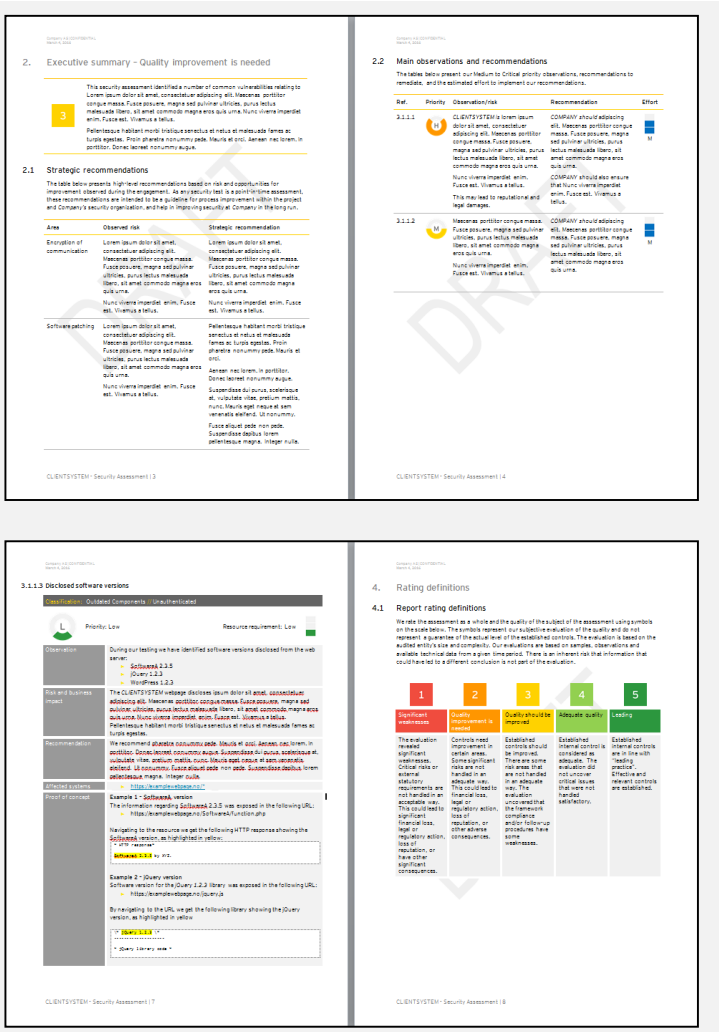
Figuren nedenfor viser hvordan et testscenario ofte forløper seg. Kritiske systemer kan også kartlegges tidligere avhengig av angrepsscenario.

Metode

Fra vårt nordiske sikkerhetssenter leveres årlig over 15 000 timer med tekniske sikkerhetsvurderinger, og vi har således meget god erfaring med sikkerhetstesting av webapplikasjoner, webtjenester og underliggende infrastruktur. Sammen med EYs globale fagnettverk har vi utarbeidet en testmetodikk basert på ledende praksis og blant annet standarder som OWASP ASVS og OWASP TOP 10. Prosesskartet under gir en overordnet beskrivelse av aktivitetene som vil inngå i testen. Metodikken vår er fleksibel og vil tilpasses til å etterligne angrepsteknikker som typisk benyttes av angripere som er relevante for offentlige virksomheter.

* For effektivt å kunne teste feil i applikasjonslogikk og tilgangsrettigheter er det viktig at man har testbrukere med ulike testroller tilgjengelig.

Rapportering



Det vil utarbeides en sluttrapport som dokumenterer hvilke tester og verktøy som er brukt, samt identifiserte svakheter og risikoområder. Rapporten leveres med en «ikke-teknisk» oppsummering som på et overordnet nivå forklarer hvilke observasjoner og risiko som er avdekket. Denne inkluderer også strategiske anbefalinger for å forbedre virksomhetens sikkerhetsprosesser.

- Rapporten leveres også med en detaljert beskrivelse av hvilke observasjoner, risiko og anbefalinger sikkerhetstesten avdekket. Dette inkluderer også en svært detaljert forklaring på hvordan sårbarhetene kan utnyttes slik at man senere kan reprodusere disse og sammenlikne resultat etter eventuelle endringer.
- For å kunne holde oversikt over funksjonalitet som har blitt testet i applikasjonen, vil rapporten inkludere et vedlegg som lister opp hvilken funksjonalitet, inkl. sider, funksjonskall og parameter, som har blitt testet.

Takk for oppmerksomheten

Spørsmål?

Building a better working world