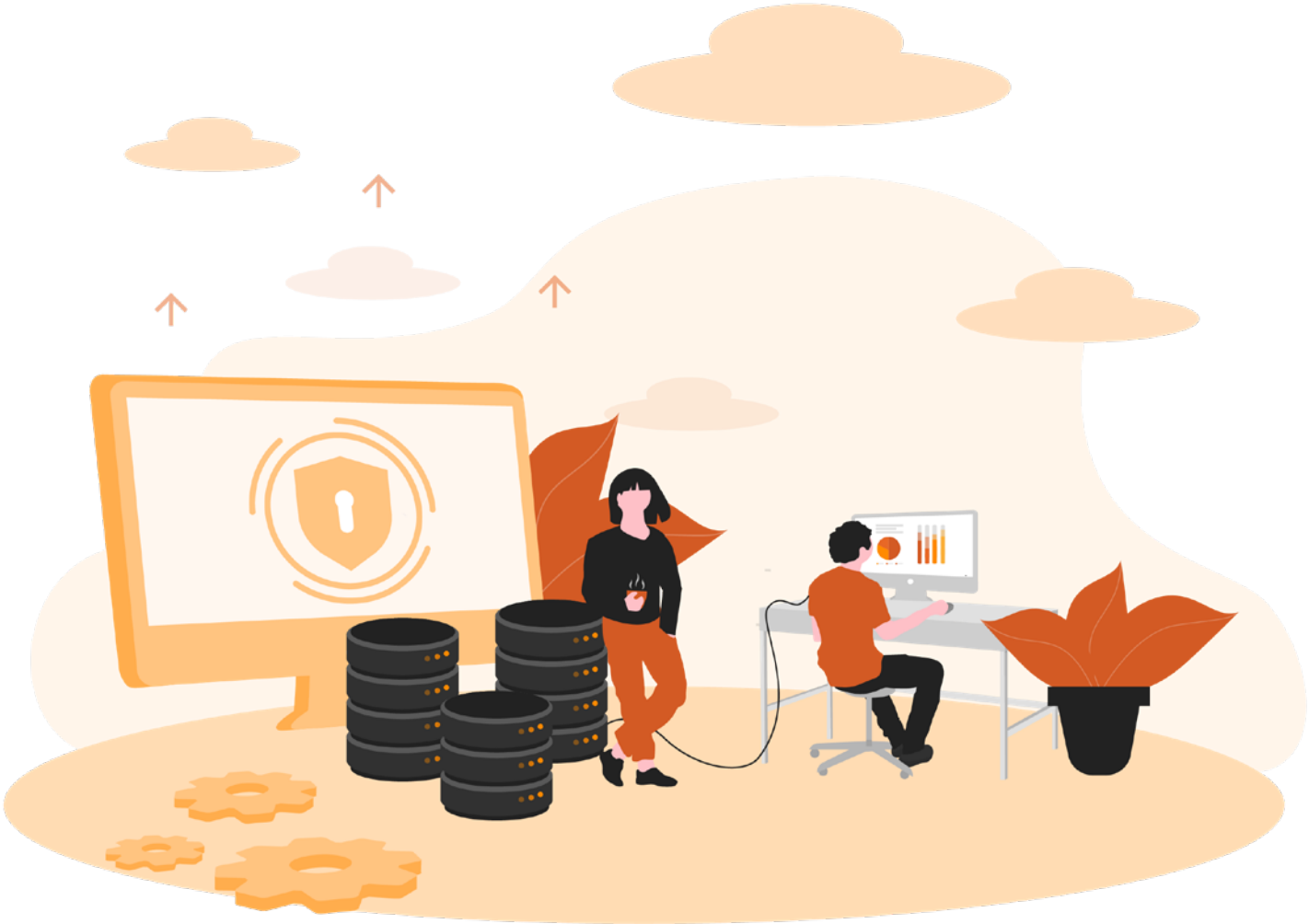
Øk datasikkerheten
i bedriften din



SNORRE data AS

Hvordan kan en god **sikkerhetskultur** hjelpe din bedrift?

De fleste bedrifter har dårlig oversikt over systemene og nettverkene som brukes, for ikke å nevne hvilke tilganger de ansatte har. Ved å gjøre datasikkerheten til en del av de daglige rutinene, blir det enklere å forholde seg til.

Norske bedrifter er et yndet mål for datakriminelle. Utad er vi oppfattet som en pengesterk nasjon. Har bedriften digitale sikkerhetshull, vil hackerne prøve å utnytte seg av det. Majoriteten vet heller ikke hvor dårlig stilt de er.

Sannheten er at det er et tidsspørsmål før de vil bli utsatt for et dataangrep. Da gjelder det å være godt rustet.

Nasjonal Sikkerhetsmyndighet (NSM) har satt opp et typisk hendelsesforløp under et dataangrep. Hvis du ikke har verktøy til å stoppe disse angrepsmetodene er du dessverre dårlig stilt. Våre IT-konsulenter vil kunne identifisere disse forsøkene gjennom såkalte penetrasjonstester. Vi avdekker sikkerhetshullene, og ser hvordan du kan tette dem.

En god sikkerhetskultur starter ved å gjøre datasikkerhet til en del av hverdagen. Det må inn i de daglige rutinene – også hos de ansatte – for å gjøre en forskjell i det store. Menneskelige feil, som å dele etpassord eller åpne en mistenkelig mail, står for 90 prosent av alle dataangrep, ifølge Verizons sikkerhetsrapport for 2019.

Nettopp derfor må du prioritere det forebyggende sikkerhetsarbeidet. Bare slik kan du redusere risikoen for et vellykket angrep.

Et typisk **hendelsesforløp**

Tiltakene er hentet fra
NSMs Grunnprinsipper 2.0.

1. PÅLOGGINGS-INFORMASJON

Aktør får tak i påloggingsinformasjon til brukerne for fjernaksessløsning ved hjelp av passorddump, kjøpt på internett eller ved Brute Force-angrep. Her vil hackerne gjette seg frem til passordet ved hjalp av kraftige datamaskiner, eller et nettverk av mange datamaskiner.

- Styr tilgang til enheter
- Bruk multi-faktor autentisering

2. LOGGER INN PÅ SYSTEMET

Aktør bruker påloggingsinformasjonen til å logge på fjernaksessløsning til virksomheten og får tilgang til virksomhetens nettverk

– *Se tiltak tillhørende punkt 1*

3. KARTLEGGER NETTVERK

Aktør gjør en initiell kartlegging, for videre å spre skadevare på virksomhetens maskiner og utstyr.

– *Del opp virksomhetens nettverk etter virksomhetens risikoprofil*
– *Kontroller dataflyt*
– *Etabler sikkerhetsovervåkning*
– *Analyser data fra sikker-hetsovervåkning*

4. UTNYTTER SÅRBARHETER

Aktør utnytter gamle, offentlig tilgjengelige sårbarheter til «glemte» enheter eller som er dårlig sikret av IT

– *Kartlegg enheter og programvare*
– *Endre alle standardpassord*
– *Ivareta en sikker konfigurasjon*
– *Etabler en sikker IKT-arkitektur*
– *Del opp virksomhetens nettverk etter virksomhetens risikoprofil*

5. FORSØKER Å FÅ TILGANG TIL VERDI

Aktøren prøver å få tilgang til virksomhetens verdier (adskilt), men lykkes ikke

– *Kontroller dataflyt*
– *Ha kontroll på identiteter og tilganger*

6. KARTLEGGER NETTVERK IGJEN

Aktøren går tilbake til første tilgangspunkt (del av kontornettverk) og kartlegger mer

- *Styr dataflyt mellom nettverkssoner*
- *Etabler sikkerhetsovervåkning*
- *Analyser data fra sikkerhetsovervåkning*

7. FINNER PASSORD OG BRUKERNAVN

Aktøren finner nettverksenhet med leverandørstandardpassord som finnes på Internett, logger på net-tverksenhet, henter konfigurering og får liste med brukernavn og passord

- *Endre alle standardpassord*
- *Kjøp moderne og oppdatert maskin- og programvare*

8. GÅR TILBAKE I NETTVERK

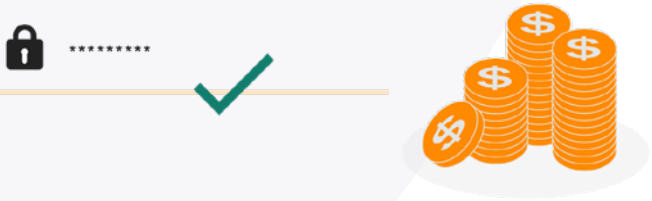
Aktøren beveger seg tilbake i nettverket via glemte enheter

- *Se tiltak punkt 3*

9. BRUKER PASSORD FOR Å FÅ TILGANG

Aktøren bruker passord hentet fra nettverksenheten og får tilgang til virksomhetens verdier

- *Ha kontroll på identiteter og tilganger*
- *Etabler retningslinjer for tilgangskontroll*



10. HENTER UT BEDRIFTENS VERDI

Aktøren kan endre/manipulere virksomhetens verdier og/eller hente ut verdiene

- *Ha kontroll på identiteter og tilganger*
- *Minimer rettigheter til sluttbrukere og spesialbrukere*
- *Identifiser virksomhetens prosesser for risikostyring knyttet til IKT*

Våre råd for **økt datasikkerhet**

1. SIKKERHETSOPPLÆRING FOR DE ANSATTE

En grunnleggende opplæring i datasikkerhet øker forståelsen.

2. OPPRETT GODE RUTINER

For å opprettholde datasikkerheten må du ha gode rutiner rundt det digitale i bedriften, også tilknyttet informasjonssikkerhet.

3. HOLD TEKNOLOGIEN OPPDATERT

Ved å bruke moderne og oppdatert program- og maskinvare er du tryggere. Det gjelder også de bærbare enhetene.

4. UTFØR JEVNLIGE SIKKERHETSANALYSER

Hold deg oppdatert på trussel-situasjonen, og gjør analysearbeid som avdekker de største risikoene.

5. INFORMASJONS-SIKKERHET I FOKUS

Som bedriftseier skal du sikre god informasjonsbehandling, i alle ledd i bedriften. Det gjelder også sikkerheten i alle IKT-systemer.

6. SIKKER SKYLAGRING

Lagring i skyen kan være riktig for deg og din bedrift. Men sørg for at løsningen er pålitelig, og at informasjonssikkerheten er ivaretatt.

7. HOLD BRANNMUREN OPPDATERT

Dette er essensielt for å sikre nettverket. Her kan din IT-konsulent hjelpe deg med beste løsning.

8. VELG SIKRE PASSORD

Dine ansatte bør ha fokus på sikre passord og rutiner rundt dette, fremfor å bytte for ofte. Det lønner seg også med to-faktorautentisering – det setter vi som et krav for god sikkerhet.

9. SIKKERHETSKOPIERING AV DATA OG INFO

Du vet aldri når noe kan gå galt. Opprett et godt system for back-up av viktig data og informasjon, slik at det ikke går tapt ved et eventuelt angrep.

10. AUTORITET OG TILGANG

Få oversikt over hvem som har tilgang til hva, og ikke minst sensitiv informasjon. Sjekk hvem som kan installere applikasjoner.

11. SÅRBARHETSTESTER

Ved å utføre penetrasjons- og sårbarhetstester ser du hvor utsatt du er for et eventuelt angrep.

12. SERTIFISERINGSBEVIS

Hvis du har iverksatt de rette tiltakene for å beskytte sensitiv informasjon mot uautorisert tilgang, kan du sertifiseres av et uavhengig sertifiseringsorgan.

SNORRE data AS

Vi hjelper deg å gjøre
bedriften din **trygg**

Les mer eller ta kontakt med oss på
snorredata.no