POLITIET

RÅD TIL VIRKSOMHET UTSATT FOR CYBERANGREP

Ved et cyberangrep må det umiddelbart iverksettes tiltak for å begrense skade og hindre ytterligere driftshindringer.

Rådene beskrevet er utformet av polititjenestepersoner med erfaring fra etterforskning av cyberkriminalitet samt informasjon fra Nasjonal sikkerhetsmyndighet (NSM), men kan ikke erstatte råd fra et profesjonelt hendelseshåndteringsselskap som har dette som sitt daglige virke.

Det er viktig å tipse eller anmelde cyberkriminalitet til politiet. Politiet ønsker å involveres tidlig ved et cyberangrep. Et tidlig samarbeid med fornærmede kan gi etterforskningen viktig informasjon som gjør politiet i stand til å sikre viktig bevis, som igjen kan bidra til å berike bildet rundt trusselaktør og motivet for angrepet. Politiet har stor forståelse for virksomhetens behov for å gjenopprette normaltilstand og vil ikke hindre en effektiv hendelseshåndtering, men vi har ofte behov for fortløpende informasjon parallelt med hendelseshåndteringen.

1. OVERSIKT

Få oversikt over situasjonen, og avdekk hvilke datamaskiner/enheter, systemer og brukerkontoer som er berørt. Gjennomgå logger og brukerkontoer for å se etter avvik og endringer utført av angriper, spesielt brukere med forhøyede rettigheter til drift.

2. SKADEBEGRENSNING

Vurder å koble fra eller stenge ned berørte systemer og isolere nettverk for å hindre ytterligere spredning av skadevare, samt hindre angriper videre adgang til andre deler av systemet. Gjennomfør tvunget passordbytte på samtlige brukerkontoer. Begrens antall brukerkontoer som har tilgang til å kjøre/eksekvere programvare. Deaktiver utdaterte påloggingsmuligheter. Vurder fare for innsidetrussel.

Hvis mulig, steng ned mulighet for ekstern tilgang til virksomhetens datasystemer. Hvis ikke det er mulig, overvåk all ekstern innkommende trafikk og blokker trafikk fra land som ikke anses som nødvendig. Overvåkning av utgående trafikk vil og kunne avdekke eventuell eksfiltrasjon/lekkasje av data.

3. VARSLE

Informer alle berørte internt og eksternt. Det er viktig at alle berørte får rett informasjon raskt. Følg rådene for varsling i "**Nødplakat for digitale angrep**" som finnes på nettstedet til Næringslivets sikkerhetsråd (Ekstern lenke: https://www.nsr-org.no/aktuelt/nodplakat). Der finnes og flere råd for håndtering og gjenoppretting.

4. SIKKERHETSKOPI

Sikre en offline kopi av eksisterende sikkerhetskopi dersom dette er lagret i skyen eller er tilgjengelig gjennom det kompromitterte systemet. Merk at siste sikkerhetskopi kan være kompromittert, så vurder å sikre en eldre sikkerhetskopi. Ved gjenoppretting, benytt kun sikkerhetskopi dere er sikker på ikke er kompromittert. Benytt oppdatert skadevare-skanner som oppdager skadevaren deres virksomhet er utsatt for.

5. SIKRE LOGGER / BEVIS

Hvis mulig, sikre all tilgjengelig informasjon om cyberangrepet, inkludert logger og annen data som kan belyse hva som har skjedd slik at virksomheten kan gjennomføre forbedringer og andre sikkerhetstiltak i etterkant. Slik informasjon er avgjørende dersom virksomheten ønsker at politiet skal etterforske cyberangrepet.

6. REDUSER RISIKO FOR NYTT ANGREP

Identifiser inngangsvektor til angriper og eventuelle svakheter/sårbarheter i virksomhetens datasystem og utbedre disse for å hindre nytt cyberangrep. Innfør minimum tofaktorsautentisering. Oppdatert infrastruktur og programvare er essensielt.