Dette dokumentet er klassifisert som TLP:GREEN. Informasjonen kan deles, men ikke publiseres offentlig. Dersom den skal refereres i offentlig publikasjon, ønsker KraftCERT beskjed.

Varsling av hendelser

Varsling av hendelser kan gjøres via skjema på https://varsling.infracert.no/, e-post til mailto:cert@kraftcert.no eller telefon til +47 940 32 443.

Send varsel

Send varsel på både faktiske kompromitteringer, angrepsforsøk og endringer i aktivitetsmønstre[1].

Send varsel i det dere oppdager en uønsket hendelse. **Ikke vent** til den er ferdig etterforsket og håndtert. Er dere usikre på om det bør varsles; send varsel! Falsk alarm er ok!

Ingen miminumskrav!

Dersom dere ikke vet mer om en hendelse enn **at det har skjedd noe uønsket**, så er det nok informasjon!

Ingen detaljkrav

Beskriv det dere vet og tror, **uansett** hvor lite det er så tidlig i et hendelsesforløp.

Listen under inneholder eksempler på nyttig informasjon som med hell kan tas med hvis mulig:

- Påvirker hendelsen daglig drift? For KBO-enheter: Påvirker hendelsen produksjon/distribusjon?
- Er det en pågående hendelse?
- Tidslinje for hendelsen. Eksempelvis når skjedde det unormale? Når ble det oppdaget?
- Hvilke soner og hvilke tjenester og systemer er berørt.
- Hva dere tror har skjedd?
- Om virksomheten har satt beredskap.
- Hvilken prosess for håndtering/etterforskning er igangsatt og ev. hvilke leverandører som er hentet inn for assistanse.
- Angrepsindikatorer (IP-adresser, domener, fil-hasher, filnavn mm).

Ingen detaljer trenger å oppgis i selve varselet. KraftCERT/InfraCERT vil opprette en dialog ved behov.

KraftCERT/InfraCERT trenger varsler

Varsling av hendelser forbedrer KraftCERT/InfraCERTs tjenester:

- Yte assistanse til virksomhetene dersom det er behov for det.
- Detektere om et angrep på en virksomhet faktisk er en del av et større angrep på tvers i sektoren eller på tvers av sektorer.
- Dele informasjon fra hendelser til resten av sektoren slik at en hendelse hos en virksomhet kan styrke sektoren på tvers.
- Bygge tilstandsbilder og statistikk som sektorene selv og ansvarlige myndigheter kan bruke i arbeidet med videre sikring og ressurstildelinger i sektorene.

KraftCERT/InfraCERT vil ikke videreformidle informasjon om enkelthendelser til tilsynsmyndigheter.

[1] For eksempel *Merkbar endring i skann-aktivitet mot en port eller addresserom*.

Eksempler

Eksempler på hendelser som ønskes varslet. Merk at dette er ikke en uttømmende liste, men eksempler ment for å demonstrere bredde og variasjon.

Merkbar endring i skann-aktivitet mot en port eller addresserom
Rekognosering
Phishing- og svindelforsøk
Forsøk på kompromittering av utstyr og brukerkontoer
Ansatte har besvart en svindel som reell situasjon
Skadevare har sluppet gjennom brannmur
Forsøk på kompromittering av tjenester som er eksponert mot internett
Gjentagende rekognosering fra samme aktør
Kort tjenestenektangrep, uten konsekvenser for kunder eller SLA-er
Klientmaskin er kompromittert/infisert med skadevare
Tjenestenektangrep som har gitt konsekvenser
Intern konto er blitt kompromittert og benyttet til å svindle andre virksomheter
Falske fakturaer av forretningsbetydelig størrelse er blitt betalt
Forretningssystemer er kryptert
Lekkasje av betydelig mengde personsensitiv informasjon iht. GDPR
Lekkasje av dokumentasjon
Rot-sertifikat er kompromittert
Nettverkskomponent er kompromittert
Krypteringsskadevare og utpressingsangrep
DDOS-angrep mot tjenester over tid som går ut over daglig drift
Lekkasje av konfigurasjoner, passord eller kraftsensitiv informasjon
MGMT-nettet er kompromittert
Active Directory er kompromittert
Det er sannsynlig at systemer som inngår i prosesskontroll er kompromittert