Netsecurity

Netsecurity Red team

Sikkerhetstesting i offentlig sektor

Hvorfor gjennomføre sikkerhetstesting?

I Netsecurity jobber vi tett sammen med kommuner, fylkeskommuner og andre offentlige organisasjoner.

Vi opplever et felles ønske om å utvikle intern sikkerhetskultur, og forstå angrepsbildet som er i konstant endring. I hverdagen erfarer vi at det er utfordrende å frigjøre tid og ressurser til å dedikere fokus på dette.

Netsecuritys Red Team hjelper derfor med å avdekke forretningsmessig risiko og tilrettelegge for kompetanseoverføring, for å kunne være i forkant av mulige hendelser.

Hva er Red Team

Netsecurity Red Team er en gruppe med høyt kvalifiserte etiske hackere, som er sertifisert som både etiske hackere og hendelseshåndterere.

Red Team er organisert som en egen enhet i selskapet, og er et spesialisert team som leverer et mangfold av tjenester innen digitale og fysiske innbrudd.

Red Team hjelper organisasjoner med å gå fra teoretiske diskusjoner om informasjonssikkerhet, til å vurdere håndfast og konkret risiko knyttet til sårbarheter. Dette gjøres ved å demonstrere at de lar seg utnytte. Funn og anbefalinger fra rapporten kan omsettes til konkrete tiltak både på teknisk og organisatorisk nivå

Erfaringer

Over det siste året har vi sett en rekke kampanjer og målrettede angrep mot kommunal og offentlig sektor. Dette er det flere grunner til, men offentlig sektor ansett som et stadig lettere mål.

Vi erfarer at kriminelle aktører ser muligheter i lys av hvordan pandemien har tvunget alle til å gjøre endringer. Dette er typisk endringer i hvordan og hvorfra vi jobber, og at det er blitt vanskeligere å ha kontroll på organisasjonen og de ansatte.
For å redusere risiko, og avdekke sårbare forhold, har vi laget noen generiske pakker for kommunal og offentlig sektor.

Målet er å gjøre det enklere å kunne iverksette forskjellige aktiviteter sammen med Netsecurity, uten at det krever mye tid eller innsats fra oppdragsgiver. Disse tjenestene kan leveres med relativt kort tid til oppstart.

Rekognosering

Rekognosering har som mål å kartlegge hvor organisasjonen kan angripes via internett. Fra en angripers ståsted benytter vi offentlig tilgjengelig informasjon for å skaffe oss oversikt over bl.a.

- IP-adresser
- Domener
- Tilgjengelige tjenester
- Nøkkelansatte
- E-post-adresser
- Kontoer på sosiale medier
- Informasjonslekkasjer (eksponerte data, lekkete brukernavn og passord)
- Ev. mobilapplikasjoner

Rapporten presenterer en prioritert oversikt over hva vi anser som mest aktuelle angrepsflater. Denne informasjon er i seg selv nyttig for kunden, da vi ofte finner informasjon om utdaterte systemer eller systemer som er eksponert ved en feil. Slik informasjon kan brukes til å lage en liste over “lavthengende frukter” som kunden ofte retter selv.

Kritiske eller sårbare systemer som blir identifisert er også gode kandidater for videre penetrasjonstesting, hvor vi simulerer hvordan organisasjonen og systemene vil kunne bli angrepet.

Innsidetesting, simulering av infisert PC

Løsepengevirus og lekkasje av sensitiv informasjon dukker stadig opp i nyhetsbildet.
Slike angrep skjer ofte ved at en ansatt blir lurt til å kjøre skadevare, som slipper angriper inn på sin egen datamaskin. En intern penetrasjonstest vil avdekke hvor godt forberedt organisasjonen er på et slikt angrep, og hvilke konsekvenser et slikt angrep vil ha.

Det er her vi virkelig ser konsekvensene av at IT-budsjett og tid er strengt begrenset, samtidig som funnene løfter sikkerheten betraktelig når de rettes.

Testen krever at Red Team får tilgang til interne nettverk og en arbeidsstasjon som angrep kan gjøres fra. Det er viktig at arbeidsstasjonen angrepene gjøres fra tilsvarer en arbeidsstasjon som brukes i det daglige arbeidet.

Phishing

En annen måte å redusere risikoen for sikkerhetshendelser forårsaket av ansatte på, er å øve på å håndtere phishing. Phishing er et uttrykk som brukes om å lure mennesker til å gi fra seg sensitiv informasjon, eller utføre uønskede handlinger elektronisk. Dette er inngangsporten for de fleste løsepengevirus.

I kombinasjon med interne oppmerksomhetskampanjer rundt temaet, kan Netsecurity gjennomføre simulert phishing for å objektivt og målbart vurdere hvor utsatt de ansatte er for slike angrep.

Dette viser sannsynlighet og risiko knyttet til slike angrep. Man kan også øve på hvordan den enkelte skal opptre, hvis man mistenker at f.eks. en e-post er et phishing-forsøk. Positivt vinklet oppmerksomhet til riktige valg i en slik situasjon er effektivt og holdningsskapende.

Netsecurity

Sentralbord:
+47 95 55 15 15

Vegard Vaage
/Leader Red Team

+47 411 42 323

vegard@netsecurity

Netsecurity

Sentralbord:
+47 95 55 15 15

Gøran Myrvold
/Leder Region Vest

+47 917 07 544

goran@netsecurity

Last ned produktblad for hendelsehåndtering

Miljøfyrtårn®

AAA HØYESTE KREDITTVERDIGHET NETSECURITY AS Orgnr: 993856886 © Bisnode 2020.06.22

Achilles Utilities NCE QUALIFIED

KVALITETSORDNING NSM ANBEFALT FOR HENDELSESHÅNDTERING

Gaselle 2016

Gasellevinner 2017

Gasellevinner 2018

Gaselle 2019

Gasellevinner 2020 Netsecurity

Om Netsecurity

Netsecurity AS (org.nr. 993 856 886) er et norsk cybersikkerhetsselskap etablert i 2009, eid av Agder Energi Venture og ansatte.
Vi leverer strategier, kompetanse, systemer, løsninger og tjenester som bidrar til at kundens forretningskritiske systemer er robuste nok til å kunne motstå og håndtere alle typer hendelser og angrep, slik at de kan arbeide sikkert på nett.

Våre ansatte er selskapets viktigste ressurs. Vi vektlegger kompetanse, integritet og kundenærhet. Vi ansetter de beste, og motiverer våre ansatte til kontinuerlig læring og forbedring.
Vi lever av vårt rykte. Vi bestreber oss på å være nære og tilgjengelige for våre kunder. Vi ønsker oss kunder hvor vi aktivt kan støtte og bistå deres forretning eller virksomhet. Hvis du velger Netsecurity skal du vite at du kan stole på oss, og får tilgang på markedets beste kompetanse, tjenester og løsninger.

Vi har over 400 kunder i hele landet innen offentlig og privat sektor. Fellesnevneren for våre kunder er at cybersikkerhet er viktig for deres virksomhet.

Netsecurity har etablert seg som en seriøs aktør i sikkerhetsmarkedet, og har vært gasellebedrift i 2016, 2017, 2018, 2019 og 2020.
Netsecurity er som eneste selskap i sin kategori godkjent av NSM for leveranse av hendelseshåndtering.

Netsecurity har et samfunns- og miljømessig ansvar. Vi ønsker å bidra til et bærekraftig samfunn og positiv verdiskaping gjennom tjenestene og løsningene vi leverer. Selskapet er sertifisert Miljøfyrtårn.
Netsecurity har etablert en formell kontrakt for sertifisering i henhold til: NS-EN ISO27001:2017. Sertifiseringsrevisjon er gjennomført i januar 2021.

Netsecurity har egne kontorer i Oslo, Bergen, Kristiansand, Grimstad og Stavanger.

/ **Netsecurity**

Oslo
Strandveien 35
1366 Lysaker

Kristiansand
Dronningensgt. 12
4630 Kristiansand

Bergen
Sandviksbodene 1
5035 Bergen

Grimstad
Bark Silas vei 5
4876 Grimstad

Sandnes
Koppholen 6
4313 Sandnes

95 55 15 15

post@netsecurity.no

www.netsecurity.no