Er jeres cyberforsvar stærkt nok?

Vores pentestere er klar til at give dig svaret, så du kan komme hackere og andre IT-kriminelle i forkøbet!

Orange Cyberdefense

Indhold

Er du bekymret for, om I har oversete sårbarheder?

Hvilke muligheder har hackerne, hvis de angriber os?

Det er spørgsmålet, mange virksomheder stiller sig selv – ikke mindst på grund af den usikkerhed, der er i verden i øjeblikket.

Det korte svar er: Lad etiske hackere teste jeres cybersikkerhed både inde- og udefra.

Kampen mod cyberkriminalitet har hårde odds

Jeres forsvar skal tage højde for et utal af lumske strategier, mens hackerne kun skal finde ét svagt punkt for at få fodfæste i jeres netværk.

AI software har sårbarheder – både kendte og ukendte. Samtidig bliver flere og flere af vores systemer integreret med hinanden via API'er. Det skaber nye muligheder – desværre også for de cyberkriminelle, som hele tiden bliver dygtigere og mere kreative. Så hvis du sommetider mærker de små hår rejse sig i nakken, forstår vi dig 100 procent.

Vi er parate til at give dig trygheden tilbage

I Norden har vi +25 pentestere, som er trænet i at tænke som rigtige hackere, og derfor kan de afsløre skjulte sårbarheder i jeres forsvar – før de bliver udnyttet af rigtige cyberkriminelle.

Tilbage til indhold

Etisk hacking hvad er det?

Pentestere kaldes også for etiske hackere, og de ligner på mange måder en ondsindet hacker. De har samme viden og anvender de samme teknikker, når de udfører deres angreb. Den store forskel er det, der motiverer dem til at bruge deres færdigheder - og den er enorm.

Hvor ondsindede hackere vælger at bruge deres viden til at begå cyberangreb for egen vindings skyld, arbejder etiske hackere sammen med virksomheder for at forhindre kriminalitet.

Ved hjælp af penetrationstests kan man bl.a. teste sikkerheden i it-systemer, netværk og applikationer, som skaber et meget værdifuldt indblik i, hvor sårbarhederne gemmer sig. Det betyder, at virksomheder og andre organisationer får langt bedre muligheder for at styrke deres sikkerhed og undgå cyberkriminalitet.

Og hvad er pentesting?

En pentest er med andre ord et simuleret cyberangreb, som har til formål at afdække ny, faktabaseret viden om jeres aktuelle sikkerhedsniveau. Gennem pentesting er det muligt at vise, hvilke muligheder rigtige cyberkriminelle har for at trænge ind i jeres infrastruktur og analysere sig frem til alle potentielle sårbarheder i udvalgte applikationer, servere eller netværkssegmenter.

Uanset hvad målet er, er vores team af erfarne pentestere klar til at hjælpe med Assume Breach af jeres Active Directory (AD). De er konstant på forkant med udviklingen, og deres metoder er baseret på enorme mængder af security intelligence, som vi indsamler over hele verden 24/7.

For at kunne udføre en penetrationstest og lave et simuleret angreb rettet mod f.eks. organisationens web-applikationer, API'er, netværk af it-systemer, mobilapplikationer eller Wifi-netværk kræver det altid virksomhedens tilladelse, for ingen organisationer kan oursource ansvaret for deres it-sikkerhed, derfor kræver det altid jeres tilladelse og accept, før vi gør noget, da ansvaret for it-sikkerheden i sidste ende altid er jeres.

Tilbage til indhold

Vores erfarne specialister

”Der findes mange gode grunde til at penteste: Fx compliance-krav, identificering af skjulte sårbarheder eller for at undersøge behovet for andre sikkerhedskontroller.

Men værdien er større end det:
Pentesting afprøver også jeres evne til at håndtere sikkerhedshændelser, styrker samarbejdet i jeres sikkerhedsteam og øger tilliden til jeres cybersikkerhed blandt kunder, partnere og medarbejdere. Pentesting kan også påvirke jeres beredskabsplaner og på den måde skabe langsigtet værdi.”

Mia Landsem

Security Consultant / Ethical Hacker / Pentester
Orange Cyberdefense

“Når jeg angriber et netværk, bruger jeg metoder, som kan være meget svære at forudsige. Især fordi jeg “misbruger” systemerne på måder, de ikke er beregnet til at håndtere. Sommetider finder jeg også på nye strategier, som virker rigtig godt. Så er dagen reddet – dét er jobtilfredshed for mig.”

Martin Christensen

Security Consultant / Ethical Hacker / Pentester
Orange Cyberdefense

“Pentests handler først og fremmest om at finde og lukke sårbarheder. Men de kan også skabe værdi på andre måder. F.eks. som et led i at overholde compliancekrav. Eller for at vise kunder og partnere – og måske også ens egen bestyrelse – at man arbejder grundigt og ansvarligt med cybersikkerheden.

Et højt sikkerhedsniveau er rygraden i enhver stærk virksomhedsprofil, og set i den sammenhæng sender løbende pentesting et klart og proaktivt signal til alle om, at man tager it-sikkerheden alvorligt.”

Ulrik Ledertoug

Director of Business Development
Orange Cyberdefense

Tilbage til indhold

Derfor skal du lade dit netværk, dine IT-systemer og applikationer penteste

En pentest er kun så god som dem, der angriber jer. Vi råder over nogle af markedets bedste og mest erfarne specialister, som ved alt om, hvor de skal lede efter sprækker i jeres forsvar.

- **Markant lavere risiko for angreb**
  Ved at efterligne hackernes angrebsmønstre kan en pentester hjælpe jer med at minimere jeres angrebsflader.
- **Effektiv analyse – helt ud i alle hjørner**
  Vores pentestere bruger de nyeste metoder og værktøjer til at afsløre alle skjulte sårbarheder.
- **Skarp prioritering af jeres risici**
  Vores pentestere kan eliminere mange falske positiver og fokuserer på de sikkerhedsområder, der betyder mest for jeres forretning.
- **Kreative metoder**
  Vores pentestere tænker og agerer som rigtige hackere, og kan derfor identificere komplekse sårbarheder langt bedre end automatiserede scanningsværktøjer.
- **Intelligence-baseret tilgang**
  Vores pentesting er baseret på indsamling af store mængder af sikkerhedsdata fra vores 17 SOCs, 13 CyberSOCs, 8 CERT teams og 4 Scrubbing centre, identificerer og analyserer mere end 50 milliarder logs og hændelser hver dag.
- **Fuld compliance**
  Vi følger anerkendte sikkerhedsstandarder. Herunder OSSTMM, NIST og OWASP ASVS testguides.

Tilbage til indhold

Vi dækker alle behov

Uanset hvilke former for pentesting I har brug for, kan vi sammensætte det rigtige hold af specialister.

- Web Apps
- Cloud Reviews
- Wireless
- API
- Mobile Apps
- Active Directory (AD)
- Adhoc
- Build Reviews
- Infrastructure

Tilbage til indhold

Vores pentest-metode i seks trin

1

Indsamling af oplysninger

Vi identificerer og indsamler så mange oplysninger om målet som muligt. Enten ved at søge i offentlig tilgængelig information eller ved at overvåge trafik i netværket.

2

Kortlægning af trusselsbilledet

Vi identificerer og kortlægger mulige trusler mod de applikationer og/eller systemer, der skal pentestes.

3

Sårbarhedsanalyse

Vi gennemfører automatiserede og manuelle analyser af de udpegede applikationer og/eller systemer for at finde sårbarheder.

4

Angreb på svage punkter

Vores pentestere går målrettet efter at udnytte de fundne sårbarheder til at få adgang til fortrolige oplysninger eller beskyttede dele af netværket.

5

Udvidelse af angreb

Når vi har udnyttet identificerede sårbarheder og nået vores mål, udvider vi angrebet for at undersøge, om vi kan komme videre til andre dele af netværket. F.eks. ved opskalering af brugerrettigheder.

6

Rapportering

Når pentesten er gennemført, dokumenterer vi resultaterne i en rapport, som også beskriver alle relevante løsnings-forslag. Finder vi særlig farlige sårbarheder, rapporteres de øjeblikkeligt.

Tilbage til indhold

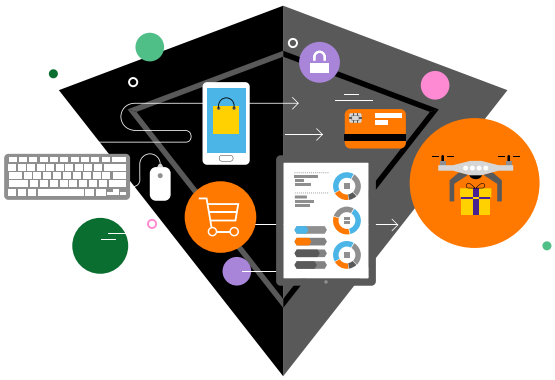
Forsvar og angreb er to meget forskellige discipliner

I de senere år er verden ikke ligefrem blevet et mere sikkert sted at drive forretning. Cyberkriminaliteten vokser, og det samme gør risikoen for digital krigsførelse.

Jo mere I ved om fjendens strategier, jo bedre kan I tilpasse jeres forsvar – og her er pentesting et yderst effektivt værktøj.

En ting er at bygge et robust cyberforsvar op indefra – noget helt andet er at teste det med angribernes metoder og værktøjer. Det er derfor simulering af ondsindede hackerangreb kan afsløre skjulte sprækker i jeres forsvar, som næsten er umulige at opdage på andre måder.

"Først går vi typisk efter at finde sårbarheder i de angrebsflader, der vender ud mod internettet. Dernæst anbefaler vi, at der også udføres pentest af det interne netværk. En realistisk risikovurdering kræver, at man ved, hvor man er mest sårbar", siger Ulrik Ledertoug, Director of Business Development i Orange Cyberdefense.



Alle sårbarheder vurderes grundigt

Når en pentest er gennemført, samles alle identificerede sårbarheder i en overskuelig rapport, hvor de vurderes på en risikoskala fra 0 til 10 af hensyn til prioritering (OWASP) – f.eks. for web-applikationer. Samtidig giver rapporten klare instrukser i, hvordan de kan fjernes.

Red teaming simulerer fuldt angreb

Hvis et cyberforsvar skal testes under maksimalt pres, kan det gøres ved hjælp af en red teaming-øvelse. Her forsøger et "rødt hold" af professionelle pentestere at angribe netværket, mens et "blåt hold" forsvarer det.

"Pentesting og red teaming fungerer forskelligt. Under pentest angriber vi typisk udvalgte servere, men i red teaming er alle servere og systemer mål for vores angreb. Så vi bygger videre på de sårbarheder, vi finder, og bruger dem til at eskalere brugerrettigheder og trænge længere ind i netværket", siger Martin Christensen, pentester hos Orange Cyberdefense Danmark.

"Ofte er det en række af små fejl eller forglemmelser, der tilsammen skaber et alvorligt sikkerhedsproblem. De kan være utrolig lette at overse – men ikke hvis man ved, hvor man skal lede."

Vi kan sætte det rigtige hold

I både Danmark, Norge og Sverige har Orange Cyberdefense opbygget stærke hold af pentestere, og derfor kan vi bemande røde hold med specialister, som nøjagtigt ved, hvordan de skal angribe de infrastrukturer, I har brug for at få testet. Undervejs følger vi brancheledende metoder som cloud best practices, CREST og MITRE.

"Red teaming giver et fantastisk godt indblik i, hvad der sker, når et angreb finder sted. Alt logges, så vi bagefter kan udføre en detaljeret analyse af, hvor og hvordan forsvaret bør styrkes", forklarer Ulrik Ledertoug.

Tilbage til indhold

Sådan brød vi ind i en kundes netværk

Opgaven lød:

“Brug alle midler til at skaffe jer fuld adgang til vores netværk ude fra - via internettet.” Herefter gik vores pentestere igang med at løse opgaven ved hjælp af følgende handlinger:

Hvad kunne domænet fortælle os?
Et hurtigt kig på crt.sh afslørede, at der var flere websites under kundens domæne. Nogle af dem var ikke blevet patchet i årevis. Efter et par requests kunne vi sende kommandoer til operativsystemet på en af kundens webservere.

Stol trygt på os, lille webserver...
Nu kunne vi ubemærket installere en web shell og en proxy, for i kundens antimalware-løsning var der lavet en undtagelse for web root directory. Desuden var systemet ikke integreret i SIEM.

Alt for nemt at finde passwords
Næste skridt var at komme uden om firewall’ens DMZ-regler. Her fandt vi igen nogle undtagelser, som gav adgang en hel vifte af password-beskyttede systemer. Så vi gav os til at lede efter passwords i interne text- og SharePoint-filer.

Næsten i mål
Ret hurtigt fandt vi flere passwords, som var skrevet ned, fordi de blev delt af flere brugere. Da vi først var logget ind, kunne vi udtrække cleartext-passwords til flere vigtige service accounts fra QA-systemets registry.

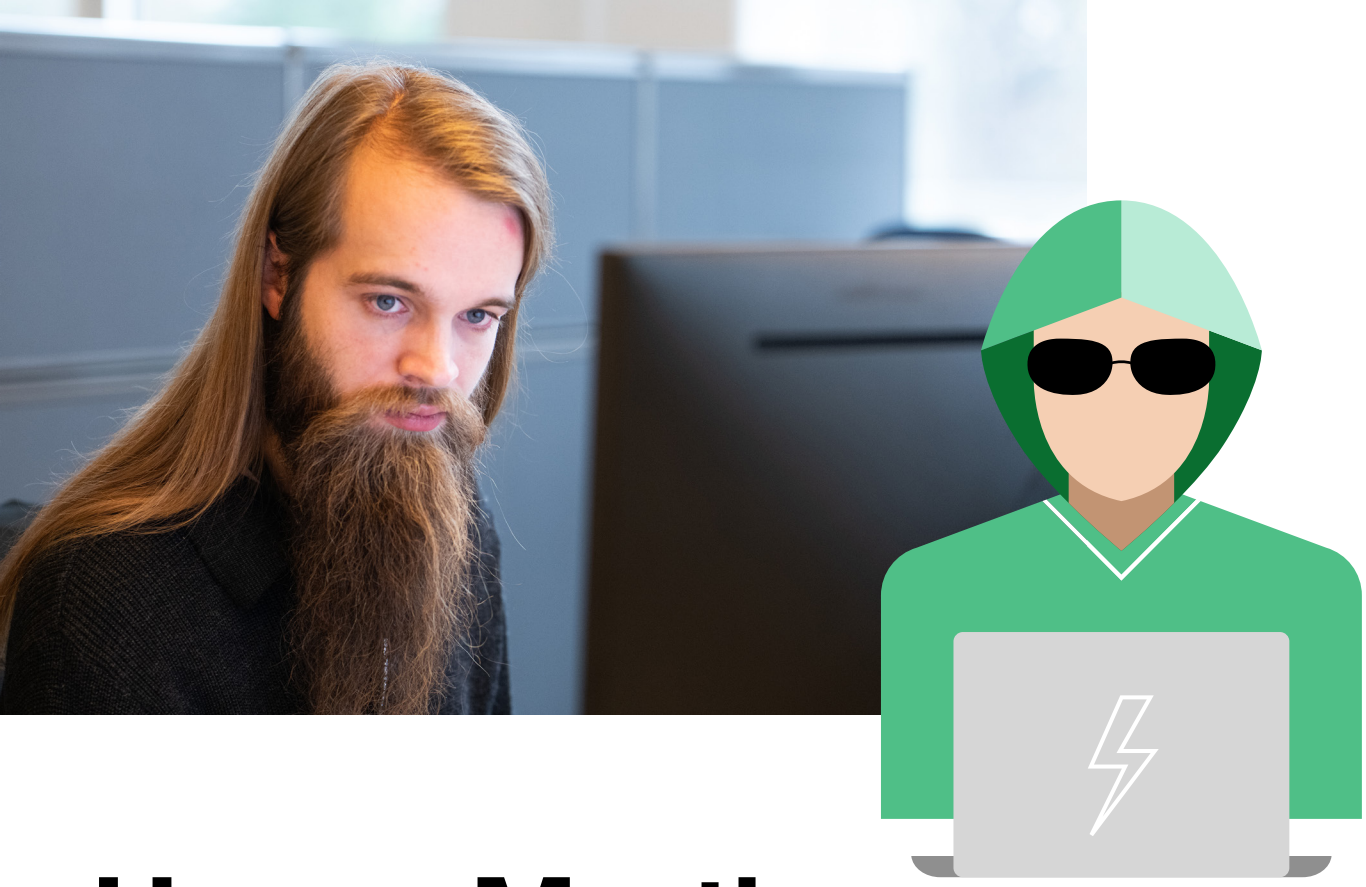
Skakmat
En af de service accounts, vi fik adgang til, blev brugt af en forretningskritisk løsning med domain administrator access. Og så var spillet ude – vi havde opnået fuld adgang til netværket.

* * * _

Hvilke indsigter fik kunden ud af angrebet

- At en kæde af “harmløse” undtagelser kan skabe et alvorligt sikkerhedsproblem
- At ingen systemer er mindre vigtige. Test- og demo-miljøer bør beskyttes på linje med produktion
- At fuld monitorering er vigtig: SOC og SIEM må ikke have blinde vinkler
- At passwords ikke bør deles. Hvis det virkelig er nødvendigt, bør de opbevares krypteret og sikkert

Tilbage til indhold



Her er Martin - han er jeres netværks bedste fjende

Èn af verdens bedste etiske hackere

Arbejdet som pentester kræver stor viden og lyst til at tænke ud af boksen. Disse evner besidder Martin Christensen – der er Security Consultant i Orange Cyberdefense – i en sådan grad, at det har bragt ham højt op på ranglisten over verdens allerbedste etiske hackere. Så spørgsmålet er: Kan jeres forsvar holde ham ude?

Jager sikkerhedshuller

“Som etisk hacker skal man have gode analytiske evner og vide rigtig meget om de systemer og programmeringssprog, man angriber. Man skal også have et slags jagtinstinkt. Man skal synes, at jagten på sikkerhedshuller er det sjove, og at regler er til for at blive brudt”, forklarer Martin Christensen.

Udfordring at sætte sig i hackernes sted

En af de helt store udfordringer ved at sætte sig i hackernes sted er nemlig, at de tænker anderledes end programmører og interne sikkerhedsmedarbejdere. I stedet for at følge regler og procedurer fokuserer hackere på at bryde dem for at finde veje ind i beskyttede netværk med store digitale værdier.

Sløset programmering skaber sårbarheder

Skjulte sårbarheder kan ofte tilskrives manglende opdateringer, dårlig kode eller forkerte konfigurationer. Et klassisk eksempel er, at en hacker kan forsøge at uploade kode via dialogfelter på et website. Hvis sitet ikke er programmeret til at forhindre det, kan hackeren få adgang til webserveren og derfra til resten af netværket.

Benytter uforudsigelige metoder

“Når jeg angriber et netværk, bruger jeg metoder, som er svære at forudsige. Især fordi jeg “misbruger” systemerne på måder, de ikke er beregnet til at håndtere. Sommetider finder jeg også på helt nye strategier, som afslører alvorlige sikkerhedsproblemer. Når det sker, er dagen reddet – dét er jobtilfredshed for mig”, fortæller Martin.

Tilbage til indhold

Brage kan hacke din virksomhed og det bør du være glad for

Brage Celius er etisk hacker hos Orange Cyberdefense, og for ham er pentesting altid en spændende udfordring. Især når han skal trænge ind i systemer eller applikationer, som forventes at være helt sikre. Her lykkes det ofte for Brage at komme forbi alle sikkerhedslag alligevel.

”Udover at det giver mig et personligt kick at hacke mig igennem en virksomheds, på papiret, ”sikre” systemer, netværk eller applikationer, så giver det også masser af værdi for kunderne, fordi jeg helt tydeligt viser dem, hvor de er sårbare, og herefter kan mine kolleger rådgive dem om, hvordan de lukker sikkerhedshullet”, forklarer Brage.

En penetrationstest kan være mange forskellige ting

På en typisk arbejdsdag er Brage enten på opgave for en kunde, eller også arbejder han med at forbedre sin egen ekspertise. Opgaverne kan vare fra en dag til flere uger, og de kan være meget forskellige fra hinanden. De udføres enten fra kontoret eller ude hos kunden. Det afhænger af opgavetypen.

Hvad skal der til for at blive en god pentester?

For at få succes som etisk hacker eller penetrationstester skal man være i besiddelse af en stor portion nysgerrighed og være motiveret af at gøre en forskel for kunderne.

”Som pentester støder du konstant på ny teknologi og bliver hele tiden eksponeret for situationer, du ikke har stået i før. Derfor er det vigtigt at kunne tilegne sig viden hurtigt og forstå, hvordan tingene fungerer. Ofte er de sårbarheder, vi afdækker, ikke noget man kan søge efter på internettet, fordi mange kunders systemer er unikke. Derfor skal du også have en god portion logisk sans. Det er nok en af de mest fremtrædende egenskaber hos en rigtig god penetrationstester”, forklarer Brage.

Stærke ressourcer til at udføre alle slags angreb

Brage har arbejdet med forskellige aspekter af it- og informationssikkerhed, inden han besluttede sig for at fordybe sig i penetrationstest – og det var ikke hvem som helst, han ville arbejde for

”Som Europas største udbyder af cybersikkerhedstjenester har Orange Cyberdefense en bredde og en trusselsindsigt, der i mine øjne er svær for konkurrenterne at matche. Med over 150 dedikerede penetrationstestere over hele verden har vi ekspertisen til at udføre angreb af alle slags og omfang. Uanset hvad vores kunder ønsker at få testet, så er vi parate og i stand til at udføre opgaven”, siger Brage og fortsætter:

“I Orange Cyberdefense har jeg alle muligheder for at være blandt de bedste inden for mit felt, fordi jeg hele tiden bliver udfordret. Det er et meget fagligt udviklende miljø at være i, og det er utroligt spændende.”

Tilbage til indhold

Fem af de mest effektive angrebsmetoder

I Orange Cyberdefense analyser vi konstant på enorme mængder af sikkerhedsdata fra hele verden. Resultaterne formidles direkte videre til vores pentestere på daglig basis.

1. Phishing
Falske emails med link til malware er en velkendt strategi – men den virker stadig.

2. Skanning efter kendte sårbarheder
Vi identificerer og kortlægger mulige trusler mod de applikationer og/eller systemer, der skal pentestes.

3. Usikre webservere
De fleste websites har dialog-felter til upload af data. Men hvis sikkerheden omkring dem er svag, kan de bruges til upload af kode, der skaffer adgang til webserveren og derfra til resten af netværket.

4. Usikre hjemmearbejdspladser
Varierende hardware, flere brugere, besøg på usikre websites, brug af ubeskyttede USB-sticks. Listen over mulige sikkerhedsproblemer i hjemmearbejdspladser er lang. Det ved hackerne, og det bruger de til deres fordel.

5. Supply Chain-angreb
Her inficeres opdateringer fra kendte software-leverandører, så hackernes malware rejser med som "blind passager" i normale opdateringer. Denne metode er særlig effektiv, fordi den misbruger eksisterende tillidsforhold til partnere eller leverandører.

Tilbage til indhold

Orange Cyberdefense

- **Orange Cyberdefense** er en af Europas ledende it-sikkerhedsleverandører med mere end 25 års erfaring inden for cybersecurity og Managed Security Services. Vores kompetencer spænder over alt fra overvågning, pentesting, analyse, rådgivning og sparring til implementering, drift og administration af kundernes strategiske it-sikkerhedsløsninger.
- **Orange Cyberdefense** er eksperter i at analysere virksomheders, myndigheders og organisationers it-sikkerhed og rådgive om, hvordan man bedst prioriterer de nødvendige indsatsområder i forhold til det aktuelle trusselsbillede.
- **Orange Cyberdefense** råder over 250 af branchens bedste analytikere fordelt på 17 SOCs, 13 CyberSOCs og 4 CERTs i hele verden. De indsamler og analyserer data fra over 500 informationskilder 24/7, hvilket giver markedets bedste intelligence-baserede billede af, hvordan det globale trusselsniveau udvikler sig.
- **Orange Cyberdefense** har et stort og internationalt white hat hacker-team, som består af 150 etiske hackere, hvoraf +25 sidder i Norden.

Kontakt os hvis du har spørgsmål, brug for rådgivning eller hjælp til pentest.

Send e-mail

Tilbage til indhold