2021

Kodeks for gennemførsel af sikkerhedstests

2021

Med den omfattende digitalisering af både erhvervslivet, den offentlige sektor og befolkningen stiger risikoen for og konsekvenserne ved cyberkriminalitet.

Skal vi høste de digitale gevinster, er det nødvendigt at virksomheder og borgere kan bevare tilliden til digitalisering, at de forstår den digitale verden og er opmærksomme på dens faldgruber.

For at sikre sig at man har tilstrækkelig beskyttelse af sin organisation eller virksomhed, er det afgørende med jævne mellemrum at teste sin sikkerhed for at identificere og rette sårbarheder.

En sikkerhedstest kan foregå på mange forskellige måder, og bør som udgangspunkt bruge nogle af de samme værktøjer og teknikker, som en fjendtlig aktør ville bruge. Men en sikkerhedstest må aldrig krænke eller udstille enkelte medarbejdere.

Når man gennemfører sikkerhedstest, ved at agere fjendtlig aktør, kan der uforvarende opstå situationer, hvor den der sikkerhedstester risikerer at komme på kant med juridiske og etiske grænser for, hvad man må og bør gøre som led i at teste sikkerheden.

For at imødegå denne usikkerhed, og for at bidrage til at en sikkerhedstest udføres med respekt for de etiske rammer og medarbejdernes hverdag og privatliv, har IT-Branchen, KL og HK i fællesskab udarbejdet dette kodeks for udførelse af sikkerhedstests.

Med dette fælles kodeks opstilles en række spilleregler, som både de leverandører der gennemfører testen, de der bestiller testen, og de der bliver berørt af testen med fordel, kan anvende.

Kodekset afsendes af en lang række organisationer der alle støtter kodekset og vil arbejde for at kodekset anvendes i forbindelse med gennemførelse af kommende sikkerhedstests. Kodeksets afsendere er:

Akademikerne

Center for Cybersikkerhed

Dansk Erhverv

Dansk Industri

Danske Regioner

Digitaliseringsstyrelsen

Erhvervsstyrelsen

HK

IT-Branchen

KL

SMVdanmark

Hvad skal kodekset?

Kodekset skal ses som en række minimumsforpligtelser til leverandører af sikkerhedstests og deres kunder.

Kodeksets primære fokus er retningslinjer, som ikke er reguleret ved lov. Kodekset er ikke en juridisk vejledning, men indeholder dog en række henvisninger til relevant lovgivning, der bør tages i betragtning. Inden gennemførsel af en sikkerhedstest er det afgørende at kunden og leverandøren sammen gennemgår relevant lovgivning og relevante aftaler der kan have betydning for testen.

Kodekset er ikke en certificerings- eller en mærkningsordning, men det er tanken, at leverandører af sikkerhedstest og deres kunder skal kunne anvende kodekset til en dialog om fælles forståelse af, hvad der er god praksis i forbindelse med sikkerhedstest.

Begrebsafklaring

Forskellige typer af sikkerhedstests går under mange navne, blandt andet penetrationstest, red team test, sikkerhedstekniske undersøgelser mv. Vi har valgt i dette kodeks at bruge det brede begreb *sikkerhedstest*, dog vil enkelte af anbefalingerne forholder sig mere snævert til specifikke typer af sikkerhedstest.

Der er mange metoder til at til at gennemføre sikkerhedstest, fx:

- Hacking, hvor den digitale sikkerhed testes gennem angreb på it-udstyr
- Phishing, hvor medarbejdere digitalt fx via e-mails lokkes til at afgive bl.a. brugernavn og adgangskode eller trykke på kompromitterende links
- Social engineering, hvor kundens medarbejdere lokkes til at afgive oplysninger eller give adgang til systemer

Ofte vil flere af ovenstående metoder bliver brugt i sammenhæng. Kodekset er som minimum relevant for alle disse typer af sikkerhedstest.

I den følgende tekst vil organisationen, som har bestilt sikkerhedstesten, blive beskrevet som *kunden*, mens virksomheden, som leverer sikkerhedstesten, beskrives som *leverandøren*.

2021

6 principper for sikkerhedstest

1

Vær enige om mål og midler

Leverandøren og kunden bør indgå klare aftaler, der beskriver opgavens formål og metode. Aftalen bør som minimum afklare:

- hvilke aktivitetstyper leverandøren må anvende – social engineering, phishing, hacking mv.
- hvordan leverandørens arbejde dokumenteres – må der fx bruges video- eller lydoptagelser?
- hvilke systemer og dele af arkitekturen samt afdeling, funktion eller fysisk lokation, som er målet for testen, og om der er specifikke systemer, afdelinger, medarbejdere eller lokationer, som skal undtages fra testen

Der bør være proportionalitet mellem mål og midler, og leverandøren bør som udgangspunkt ikke anvende mere indgribende metoder end nødvendigt.

Leverandøren bør sikre, at kundens ønsker ikke er i strid med principperne i dette kodeks.

1.1 Søg opbakning til testen

Da en sikkerhedstest kan berøre mange af kundens medarbejdere, kan det være en god ide at sikre, at der er opbakning til testen hos kundens øverste ledelse. Det er naturligvis kundens ansvar at sikre, at der er denne opbakning, og det vil være god skik, at leverandøren spørger ind til det inden underskrift på aftalen.

2

Test organisationen, ikke medarbejderen

Det må aldrig være formålet med en sikkerhedstest at udstille medarbejderes fejl eller ageren, men alene at teste organisationens, organisatoriske eller tekniske sikkerhed.

2.1. Medarbejderstaben skal varsles

Inden der gennemføres en sikkerhedstest, som berører medarbejderne, anbefales det, at medarbejderne informeres om, at der i den kommende tid vil blive udført test af virksomhedens sikkerhed, for at undersøge sårbarhed overfor eksterne trusler.

Hvis sikkerhedstesten skal give mening, bør orienteringen være tilpas generel og tidsmæssigt bred for ikke at påvirke medarbejdernes ageren unødigt. Kunden kan med fordel overveje at indskrive denne orientering i virksomhedens retningslinjer, medarbejderhåndbog, intranet eller lignende.

På visse arbejdspladser og i overenskomster kan der være indgået aftaler, der begrænser muligheden for at gennemføre ikke-varslede tests. Det er til enhver tid kundens ansvar at kende til og overholde sådanne aftaler, men leverandøren bør aktivt spørge ind til, om der er særlige aftaler herom, som skal overholdes.

2.2 Afrapporteringen må ikke udstille medarbejdere

For at sikre anonymitet, bør leverandørens afrapportering til kunden ikke indeholde oplysninger om specifikke medarbejdere eller meget små grupper af medarbejdere, hvor enkeltpersoner vil kunne identificeres. Anbefalingerne til kunden bør ligeledes aldrig være rettet mod navngivne medarbejdere.

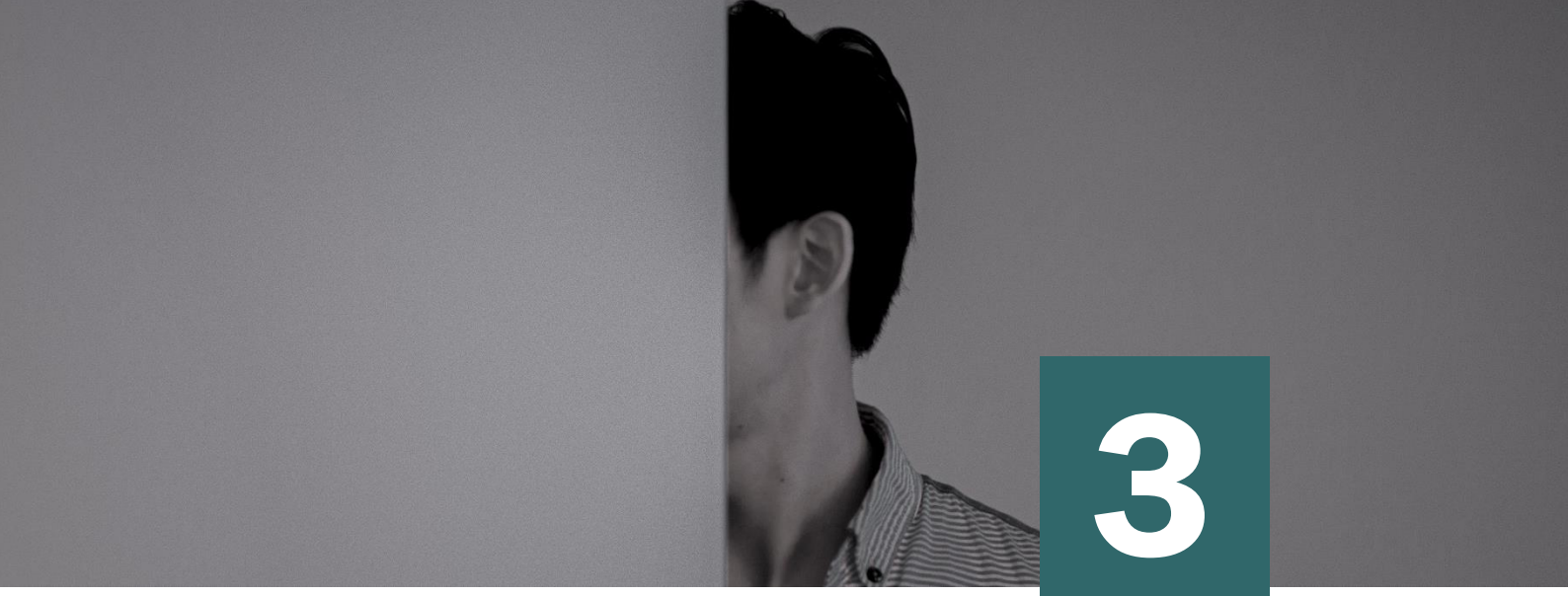
2.3 Video- og audio-materiale bør ikke videregives

Video- og audiomateriale kan være god dokumentation for det udførte arbejde og de identificerede sikkerhedsudfordringer.

Leverandøren bør ikke videregive video- og audiomateriale indeholdende identificerbare personer til kunden. Anvendelse af dette materiale bør kun ske i forbindelse med intern dokumentation - herunder afklaring af evt. tvister.

Video- og audiodokumentation af f.eks. adgang, udstyr og funktioner hos kunden kan videregives til kunden, så længe det ikke indeholder personer. Leverandøren bør endvidere være opmærksom på at overholde lov om TV-overvågning.

Opbevaring og slettefrister skal som min. overholde gældende lovgivning, og bør aftales med kunden inden underskrift af kontrakt.



3

Indhold og brug af case-materiale

Gennemførslen af en sikkerhedstest vil ofte kræve, at leverandøren – ligesom en fjendtlig aktør – udgiver sig for at være en anden eller bruger en usand fortælling til at få adgang til ellers utilgængelige systemer. Leverandøren bør udelukkende bruge dette redskab, når det skønnes nødvendigt for gennemførslen af testen. Leverandøren skal på forhånd afklare indholdet og brug af case-materialet med kunden.

3.1 Hvem må man udgive sig for at være?

Leverandøren bør altid have klare aftaler med kunden om, hvem man må udgive sig for at være, herunder om man må udgive sig for at være en anden person fra kundens egen organisation.

Leverandøren kan grundet lovgivning aldrig udgive sig for at være en myndighedsperson, som fx fra politiet, Datatilsynet eller skattevæsnet.

Endvidere er det god skik, at leverandøren ikke udgiver sig for at være en repræsentant for eksisterende 3. virksomhed, med mindre der foreligger en aftale med den pågældende virksomhed.

3.2 Phishing

Ved anvendelse af phishingkampagner er det afgørende, at leverandøren aftaler med kunden, hvordan man forsøger at få oplysninger ud af kundens medarbejdere. Kunden bør således godkende en konkret case-beskrivelse af phishingkampagnen inden udsendelse.

Leverandøren bør på ingen måde sprede misinformation om kunden. Man skal være særligt varsom med at sprede falske historier, da det kan have store økonomiske konsekvenser eller påvirke kundens omdømme.

4

Giv dig til kende i tilfælde af konflikter

Det er ikke utænkeligt, at der kan opstå konflikt i forbindelse med gennemførsel af en sikkerhedstest. Det kan fx være medarbejdere med mistanke til leverandøren, der forsøger at forhindre leverandøren i at gennemføre testen.

Kunden og leverandøren bør derfor lave aftaler der gør det klart hvor langt leverandøren må gå for at skjule sin identitet, og hvornår leverandøren skal give sig til kende og afsløre formålet med sin tilstedeværelse. Man bør i den sammenhæng være opmærksom på at der kan være andre end kundens medarbejdere på lokationen, fx kunder, gæster, håndværkere og lignende, som evt. skal behandles anderledes end kundens egne medarbejdere.

4.1 Lav klare aftaler om, hvem der skal kontaktes

Det anbefales at have nogle meget klare aftaler på plads mellem kunde og leverandør inden gennemførsel af testen om, hvem man kontakter i tilfælde af konflikt. Dette vil medvirke til at sikre, at kunden er orienteret om konflikten, og at konflikten ikke udvikler sig. Kontaktpersonen bør være en person med tilstrækkelig beslutningskompetence, som er grundigt orienteret om testens gennemførsel, og som bør være tilgængelig under hele testens gennemførsel.

Det anbefales endvidere at det aftales mellem kunde og leverandør, hvem der skal kontaktes i tilfælde af, at en medarbejder oplever sikkerhedstesten som grænseoverskridende adfærd. Dette kan med fordel være en relevant medarbejder med HR-funktioner.

5

Videregiv viden om kriminelle handlinger

Det er ikke formålet med en sikkerhedstest at afsløre kriminelle handlinger, men hvis leverandøren i forbindelse med en test opdager kriminelle handlinger, bør leverandøren straks reagere.

Er der tale om personfarlig kriminalitet, bør leverandøren uden ophold anmelde det til politiet og orientere kunden omkring forholdene. Opdages anden kriminalitet bør leverandøren rapportere dette til kunden, som efterfølgende har ansvaret for at håndtere situationen.

6

Sørg for ansvarlig datahåndtering

Ved gennemførsel af en sikkerhedstest kan leverandøren komme i besiddelse af særligt følsomme data, som fx bruger-passwords. Følsomme data bør aldrig videregives til kunden. Vær i denne forbindelse særligt opmærksom på at overholde Databeskyttelseslovens regler, herunder slettefrister.

Det er væsentligt at få afklaret dataansvaret for indsamlede data, herunder om leverandøren er dataansvarlig eller databehandler, da det kan være relevant at indgå en databehandleraftale, således at der er klarhed over og enighed om, hvordan data håndteres, opbevares og slettes.

Materiale, som er mærket ”privat”, bør aldrig gøres til genstand for sikkerhedstesten.

Endelig bør leverandøren og kunden, aftale hvordan der skal ryddes op efter sikkerhedstesten, herunder bl.a. sletning af filer som er oprettet eller ændret af leverandøren og nulstilling af passwords.