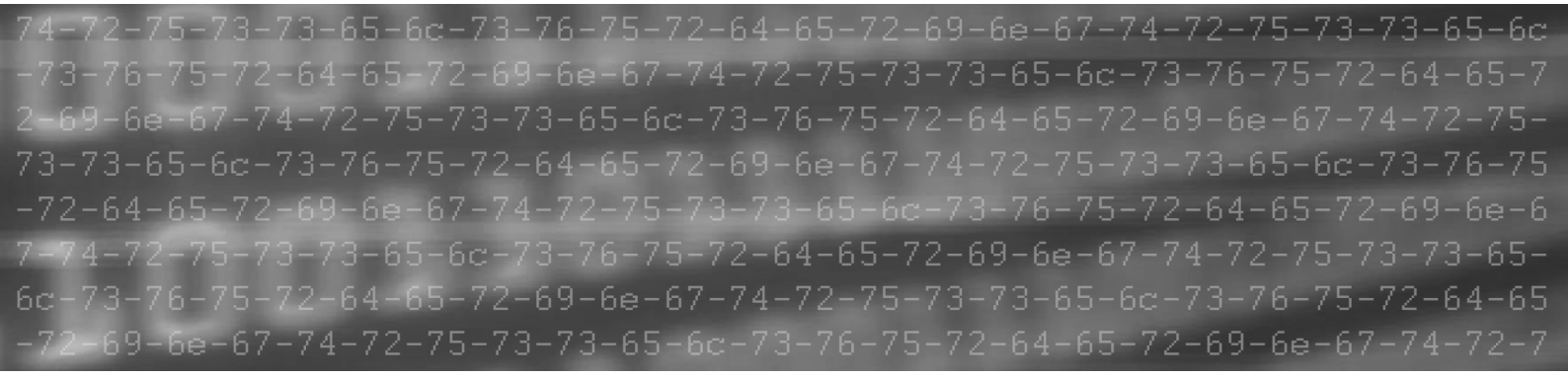
CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen fra bevidste og ubevidste insidere



Trusselsvurderingsenheden ved Center for Cybersikkerhed

Februar 2019

Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Telefon: 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave
19.02.2019

Trusselsvurdering: Cybertruslen fra bevidste og ubevidste insidere

Formålet med denne trusselsvurdering er at orientere ledelsen ved myndigheder og virksomheder om truslen fra insidere med adgang til forretningskritiske it-systemer. Medarbejdere, som er uopmærksomme, uagtsomme eller har ondsindede intentioner, kan forårsage skadelige kompromitteringer af informationssikkerheden i disse organisationer.

Hovedvurdering

- Ubevidste insidere kan findes i alle organisationer, og medfører en øget sårbarhed overfor cybertrusler.
- CFCS og PET vurderer, at ubevidste insidere er involveret i op mod halvdelen af sikkerhedshændelserne i en organisation.
- Statslige aktører og cyberkriminelle udnytter ubevidste insidere i forbindelse med cyberangreb mod danske organisationer.
- Bevidste insidere er potentielt til stede i alle organisationer.
- Hovedparten af de bevidste insiderhændelser er ansporet af en konflikt med arbejdsgiveren.
- Uden effektiv adgangsstyring og logning kan det være umuligt at identificere en bevidst insider.

Indledning

Denne vurdering beskriver cybertruslen fra insidere, og er udarbejdet i samarbejde med PET. Vurderingen fokuserer primært på insiderhandlinger, som involverer data og it-systemer i myndigheder og virksomheder, herefter kaldet organisationer. I vurderingen arbejdes der med PET's definition af en insider som en person med legitim adgang, som bevidst eller ubevidst påvirker organisationens virke gennem at sprede, skade eller ændre de informationer og processer, der udgør organisationens fundament.

Insidertruslen er fra et samfundsperspektiv særlig skadelig for organisationer, som driver samfundsvigtig infrastruktur eller tjenester, håndterer følsomme data eller besidder værdifuld intellektuel ejendom.

Insidere kan inddeles i ubevidste og bevidste insidere. De ubevidste insidere er medarbejdere, der ikke er klar over, at deres adfærd kan være skadelig for organisationen. Bevidste insidere er medarbejdere, som bevidst overtræder organisationens sikkerhedspolitikker for egen vindings skyld eller med det formål at skade organisationen.

Den ubevidste insider

Alle organisationer er sårbare overfor cyberangreb i kraft af medarbejdere, som uden deres viden kan medvirke til brud på informationssikkerheden. Ligesom det gælder for sårbarheder i f.eks. software, kan en ubevidst insider medvirke til, at organisationen bliver kompromitteret. Derfor bør alle organisationer forholde sig til truslen fra ubevidste insidere.

Museum ramt af CEO-fraud

Ved at udgive sig for at være direktør for Statens Museum for Kunst lykkedes det i 2017 svindlere at få medarbejdere til i flere omgange at overføre i alt 805.000 kroner til udenlandske konti.

På baggrund af blandt andet ENISA's Threat Landscape Report for 2016 vurderer CFCS og PET, at det er sandsynligt, at ubevidste insidere kan være involveret i op mod halvdelen af alle registrerede sikkerhedshændelser i en organisation.

I gruppen af ubevidste insidere finder man blandt andet de medarbejdere, som på grund af f.eks. uklare eller manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker. Den ubevidste insider kan eksempelvis sætte et ukendt og derfor usikkert USB-stik ind i sin arbejdscomputer eller blive narret til at oplyse adgangskoder eller andre følsomme oplysninger over telefon eller e-mail til personer, som hævder at tilhøre f.eks. organisationens it-afdeling.

Phishing og spear phishing

Afsendere af falske e-mails kan via social engineering forsøge at narre modtageren til, i god tro, at foretage handlinger, som er skadelige for modtageren eller organisationen. Phishing betegner falske e-mails, der sendes bredt ud til mange modtagere, mens falske e-mails, som er målrettet udvalgte modtagere, kaldes spear phishing. Spear phishing-mails er kendetegnet ved, at afsenderen har gjort sig særlig umage for at tilpasse indholdet til den specifikke modtager.

Cyberangreb via e-mails, såkaldt phishing eller spear phishing, er en udbredt metode til at kompromittere en organisation. Det skyldes, at det er relativt let at udføre og ofte er effektivt. En ubevidst insider kan narres til at trykke på et link til en skadelig hjemmeside eller til at åbne et vedhæftet dokument, der indeholder malware.

Spear phishing mod Tryg afværget

I marts 2018 modtog fire nøglemedarbejdere ved forsikringsselskabet Tryg spear phishing-mails med malware. Formålet var sandsynligvis at opnå adgang til regnskabsoplysninger, inden de blev offentliggjort. Fordi medarbejderne var opmærksomme på faresignaler i de falske e-mails, blev angrebet afværget, uden at der skete nogen skade.

CFCS og PET vurderer, at både statslige aktører og cyberkriminelle ofte benytter phishing og spear phishing i forbindelse med cyberangreb mod danske myndigheder og virksomheder. Aktørerne forsøger blandt andet at misbruge servicemindede og loyale medarbejdere, eksempel-

vis ved at udgive sig for at være en kunde eller en ledende medarbejder, og derved få medarbejderen til at overse faresignaler i kommunikationen eller omgå sikkerhedsprocedurer. Et eksempel er CEO-fraud, hvor en kriminel aktør via forfalskede e-mails og telefonopkald forsøger at narre medarbejdere i en organisation til at overføre penge til den kriminelle. Denne type bedrageri kan give et stort udbytte uden at kræve avancerede hackerkompetencer.

Social engineering

Social engineering betyder, at en aktør ved brug af psykologiske kneb udnytter en persons vanetænkning, autoritetstro, nysgerrighed eller hjælpsomhed til at få personen til at overse faresignaler i e-mails, telefonopkald og lignende. Derved kan personen narres til at udlevere fortrolige oplysninger eller foretage andre skadelige handlinger. Som eksempel vil spear phishing-mails ofte foregive at komme fra en person, organisation eller myndighed, som modtageren har tillid til, eller indeholde links til projekter, produkter, konferencer eller dokumenter, som kan have interesse for målpersonen.

LinkedIn udnyttes til social engineering

I juni 2017 advarede den tyske efterretningstjeneste BfV om falske kinesiske profiler på LinkedIn. De falske profiler foregav at tilhøre forskere og personer ansat ved tænketanke og konsulentfirmaer. Der blev registreret mere end 10.000 forsøg på kontakt fra disse profiler til personer ansat i den tyske statsadministration.

Social engineering kræver, at angriberen har et vist kendskab til ofret, eksempelvis arbejdsgiver, kolleger, arbejdsområde, dagligdag, interesser eller omgangskreds. Den viden kan opnås ved at søge informationer på internettet, men kan også erhverves mere aggressivt ved, at aktøren under påskud af sammenfald af interesser eller fagområder skaber et tillidsforhold til offeret. Kontakten til offeret kan ske på møder og konferencer eller via sociale medier som LinkedIn og Facebook. For en angriber kan det være attraktivt at målrette spear phishing-mails til medarbejdere med beslutningskompetencer eller med administratorrettigheder til it-systemer. Denne type information er ofte tilgængelig via en organisations hjemmeside eller på LinkedIn.

Uagtsomme medarbejdere

En særlig gruppe ubevidste insidere er de uagtsomme medarbejdere, som undlader at følge gældende sikkerhedsprocedurer, fordi de føles besværlige eller unødvendige. En anden årsag kan være, at organisationen slet ikke har defineret nogen sikkerhedsprocedure, eller at procedurerne er utilstrækkelige. Medarbejderen kan eksempelvis vælge at dele sit password med kolleger, undlade at følge organisationens regler for udformning af sikre passwords, eller overføre følsomme data via private mailkonti eller usikre medier, f.eks. for at kunne arbejde hjemmefra.

Mangel på brugbare interne it-værktøjer kan få medarbejdere til at benytte usikre og uautoriserede løsninger. Det kan eksempelvis komme til udtryk ved download af ikke godkendt software eller deling af intern dokumentation via internetbaserede fildelings-løsninger udenfor organisationens kontrol. Uagtsomheden kan også medføre, at it-systemer ikke installeres og drives i forhold til organisationens sikkerhedspolitikker eller best practice.

Læge sendte ved en fejl følsomme patientdata til kriminelle

Problemer med at åbne filer i et lukket netværk førte til, at en læge ved Styrelsen for Patientsikkerhed i 2016 sendte filer med patientdata til sin private e-mail. Fordi lægen taster sin mailadresse forkert, sendes filerne til en mailserver, som sandsynligvis kontrolleres af kriminelle.

Medarbejdere under arbejdspres kan tilsidesætte sikkerhedsprocedurer, som forsinker løsningen af en opgave.

Akutte og kritiske driftsproblemer kan ligefrem gøre det nødvendigt for en medarbejder bevidst at tilsidesætte gældende sikkerhedspolitikker, som ellers ville forsinke en fejlretning. Der kan f. eks. være tale om en medarbejder, som låner en kollegas adgang til et driftssystem for at rette en fejl. Det er ikke nødvendigvis alvorligt, men kan over tid føre til en dårlig sikkerhedskultur. Organisationer bør derfor overveje, om sikkerhedsprocedurer skal indrettes til at tage højde for den slags uforudsete situationer.

Den bevidste insider

En bevidst insider kan være særlig skadelig for en organisation. Modsat udefrakommende hackere, som i mange tilfælde bliver stoppet af sikkerhedsmekanismer som firewalls, e-mailscanning og antivirusfiltre, vil en bevidst insider ofte have succes med sine handlinger. Det skyldes, at sikkerhedsmekanismerne ikke beskytter mod en insider, som ikke nødvendigvis anvender malware, men er i stand til at udføre sine handlinger alene ved at misbruge sin stilling og legitime it-adgange.

Insider dømt for tyveri af kildekode

I 2017 blev en tidligere ansat ved IBM i Kina dømt for at kopiere kildekode til virksomhedens produkter. Ifølge amerikanske myndigheder ville den ansatte benytte koden til selv at fremstille og sælge software.

Det præcise omfang af sikkerhedshændelser begået af bevidste insidere kendes ikke, og der er sandsynligvis et stort mørketal på området. Udenlandske rapporter fra sikkerhedsfirmaer viser imidlertid, at bevidste insiderhændelser er et kendt problem i mange organisationer. I en undersøgelse havde op mod halvdelen af de adspurgte organisationer oplevet mindst et tilfælde i løbet af 2017. Baseret på offentlige rapporter og hændelser, sammenholdt med data fra samarbejdspartnere, vurderer CFCS og PET, at bevidste insidere udgør en potentiel trussel i alle organisationer.

Det er ikke muligt at opstille en generel profil på en bevidst insider. En undersøgelse lavet af Carnegie Mellon University i USA viser imidlertid, at op til 80 % af de bevidste insiderhandlinger er ansporet af arbejdsrelaterede hændelser som eksempelvis afskedigelse, forflytning eller en disciplinærsag, der har skabt en konfliktsituation mellem medarbejderen og arbejdsgiveren. Som konsekvens af konflikten vælger medarbejderen at skade organisationen for at få en form for oprejsning. Eksempler på andre motiver er økonomisk vinding, idealisme eller stærk loyalitet overfor nationer, grupper eller personer udenfor virksomheden.

Ansat saboterer Citibank routere

I 2016 blev en tidligere it-administrator i amerikanske Citibank dømt for sabotage af bankens routere. Baggrunden for hændelsen var en konflikt mellem medarbejderen og ledelsen i virksomheden.

I forbindelse med brug af underleverandører og outsourcing har en organisation ofte ringe kendskab til eller indflydelse på interne forhold hos leverandøren. Organisationer bør derfor være opmærksomme på, at konflikter mellem underleverandøren og dennes medarbejdere kan opstå uden organisationens vidende, hvorved truslen fra bevidste insidere i forsyningskæden kan øges uden eller med kort varsel.

Det kan være svært at identificere en bevidst insider

En amerikansk undersøgelse fra 2015 viste, at det i mere end halvdelen af de registrerede insiderhændelser ikke var muligt med sikkerhed at identificere gerningsmanden. Typiske årsager til det er manglende eller ineffektiv adgangsstyring og logning.

Effektiv adgangsstyring begrænser antallet af medarbejdere med adgang til følsomme systemer og data, og logning kan vise, hvem der på et givet tidspunkt har tilgået de forretningskritiske systemer og data, samt hvad medarbejderen har foretaget sig.

Statslige aktører rekrutterer insidere

Nogle stater søger aktivt at rekruttere spioner i Danmark. Formålet er dels at understøtte landets økonomi ved at stjæle intellektuel ejendom, dels at indhente oplysninger af strategisk betydning for landet.

Visse stater har ligeledes en tæt forbindelse mellem efterretningstjenesten og civilbefolkningen samt en lovgivning, som forpligter borgere og private virksomheder til at støtte landets efterretningstjeneste.

Bevidste insidere er ofte involveret i tyveri af data. En insider, som ønsker at skade sin nuværende arbejdsgiver eller give sig selv eller en kommende arbejdsgiver en fordel, kan vælge at stjæle følsom information som intellektuel ejendom, kundedokumentation eller andre forretningshemmeligheder og medbringe dem til en ny arbejdsgiver. Uden effektiv logning er det svært at afsløre ulovlig kopiering af data.

En insider, som søger en økonomisk gevinst eller bliver presset til det, kan kopiere følsomme data, der kan sælges eller misbruges til økonomisk kriminalitet. En anden mulighed er at narre arbejdsgiveren til at tro, at dataene er stjålet af cyberkriminelle og kun udleveres efter betaling af en løsesum. Uden netværksovervågning, adgangsstyring og logningssystemer er det vanskeligt at påvise, om kompromitterede data er ulovligt kopieret af en medarbejder eller er stjålet af udefrakommende hackere.

En bevidst insider vil ofte udføre sine gerninger ved hjælp af den viden og de it-adgange, som knytter sig til medarbejderens job i organisationen. En it-administrator, som ønsker hævn over sin arbejdsgiver, kan derfor være særlig skadelig. Insideren kan skaffe sig adgang til følsomme data samt ændre eller afbryde forretningskritiske it-systemer og derved skade organisationens økonomi og anseelse. Hvis eventuelle logningssystemer ikke er beskyttede, så kan det endvidere være muligt for insideren at slette sine spor.

Systemadministrator dømt for hacking mod tidligere arbejdsgiver

Efter en medarbejder ved den daværende amerikanske internetudbyder PA Online i 2010 var blevet fyret, forsøgte han at tilgå virksomhedens netværk for at hente software, som medarbejderen mente at eje. Forsøget medførte, at virksomhedens systemer gik ned, hvorefter udbyderens kunder stod uden internetadgang i en uge.

Hvis medarbejdere har fjernadgang til en organisations it-system, kan det være umuligt at kontrollere, hvem som reelt benytter denne adgang eller kigger medarbejderen over skulderen. Selv ved brug af adgangskontrol og logning kan det være umuligt at afsløre, hvis en medarbejder lader tredjepart benytte sin fjernadgang til organisationens it-systemer.

Anbefalinger

CFCS og PET anbefaler alle myndigheder og virksomheder at orientere sig om truslen fra insidere og inddrage den trussel i deres løbende risikovurdering.

Selvom ubevidste insidere kan findes i alle organisationer, så er det vigtigt også at se medarbejderne som et væsentligt værn mod cybertruslen. Dette værn fungerer imidlertid kun, hvis organisationen løbende motiverer medarbejderne til at følge veldefinerede og forståelige sikkerhedsprocedurer. Organisationer bør desuden holde medarbejderne opdateret om de metoder, som trusselsaktørerne benytter samt træne dem i at se faresignalerne i f.eks. uventede kontakter, telefonopkald, e-mails og lignende. Frem for eventuelt at bebrejde medarbejdere, som bliver ofre for phishing og social engineering, bør ledelsen opfordre til åbenhed om sådanne hændelser. På den måde kan vigtig viden om truslen hurtigt deles og løbende medvirke til at øge medarbejdernes opmærksomhed og evne til at imødegå truslen.

Organisationer kan med fordel undersøge, hvor stor potentiel skade en bevidst insider i organisationen eller hos en underleverandør kan gøre blot ved at udnytte gældende processer og legitime

adgange til forretningskritiske it-systemer og data. Resultatet kan måske give anledning til at indføre eller ændre sikkerhedspolitikker, processer, tekniske sikkerhedsmekanismer eller medarbejderes adgange til og roller på kritiske it-systemer.

Antallet af medarbejdere med adgang til forretningskritiske it-systemer og data bør begrænses. Særligt bør antallet af medarbejdere med administratorrettigheder begrænses til et minimum, hvilket også bidrager til at beskytte mod udefrakommende hackere. I forbindelse med ansættelsesophør eller overgang til ny funktion er det vigtigt, at overflødige it-adgange hurtigt spærres, og at eventuelle fælles administrator- eller root-adgangskoder, som medarbejderen har kendskab til, ændres.

Nogle medarbejdere kan have den opfattelse, at alt, der ikke er forbudt, er tilladt. Derfor er det vigtigt at opstille klare regler for, hvad medarbejderne må gøre, skal gøre og ikke må gøre. Det skal sikres, at reglerne er kendte og håndhæves. En væsentlig barriere for en insider kan være erkendelsen af, at en handling strider mod interne regler og procedurer og kan få konsekvenser.

Risikoen for afsløring kan være den hindring, som får en bevidst insider til at opgive sine planer. Derfor bør organisationer, som ønsker at mitigere insidertruslen, sikre en effektiv adgangsstyring og logning på forretningskritiske it-systemer, tiltag som også medvirker til at beskytte mod udefrakommende cybertrusler. For at virke forebyggende er det vigtigt, at medarbejderne er bevidste om, at deres aktiviteter registreres og følges. Den løbende awareness kan sikres ved almindelig information, samt ved at medarbejdere kontaktes selv ved mindre hændelser som f.eks. mislykket login eller login udenfor normal arbejdstid, hændelser som også kan indikere et udefrakommende cyberangreb.

Endeligt er det vigtigt at være opmærksom på, at konflikter med medarbejdere opdages og håndteres hensigtsmæssigt, samt om der er forhold, som potentielt kan føre til en konflikt.

CFCS har udarbejdet et antal vejledninger, som også er relevante for insidertruslen:

- Cyberforsvar der virker
- Spear phishing – et voksende problem
- Logning – en del af et godt cyberforsvar

Politiets Efterretningstjeneste udbyder desuden et kursus om insidertruslen. Information om kurset kan findes via hjemmesiden pet.dk.

FE bruger denne skala for sandsynlighed i analyser: