CENTER FOR CYBERSIKKERHED

Trusselsvurdering

# Cybertruslen fra phishing-mails

# Cybertruslen fra phishing-mails

Cyberangreb, som indledes med en phishing-mail, er meget udbredte og fører til tab af penge, data og omdømme eller alvorlige kompromitteringer af it-netværket hos myndigheder og virksomheder. Det er derfor vigtigt at være opmærksom på truslen og indføre passende forholdsregler for at imødegå den.

**Hovedvurdering**

- CFCS vurderer, at phishing ved hjælp af e-mails udgør en vedvarende og alvorlig cybertrussel mod alle myndigheder, virksomheder og borgere i Danmark.
- Det er sandsynligt, at de fleste cyberangreb i dag indledes med en phishing-mail.
- CFCS vurderer, at op mod 80 procent af de e-mails en organisation modtager udefra kan være uønskede eller direkte skadelige, og at større organisationer dagligt modtager phishing-mails.
- Phishing anvendes af både cyberkriminelle og statslige hackere. CFCS vurderer, at de fleste phishing-mails udgår fra organiserede kriminelle, som også leverer infrastruktur, værktøjer og tjenester, som understøtter phishing.
- Et phishing-angreb kan potentielt skade samfundet, hvis angrebet rammer en myndighed eller virksomhed, som leverer samfundsvigtige ydelser, tjenester eller lignende.
- CFCS vurderer, at de fleste phishing-mails fungerer i samspil med en skadelig hjemmeside, der efterligner en legitim hjemmeside. Ved at lukke eller blokere adgangen til hjemmesiden kan den skadelige effekt af den specifikke phishing-mail fjernes.

**Analyse**

CFCS vurderer, at phishing via e-mails udgør en vedvarende og alvorlig trussel mod alle myndigheder, virksomheder og borgere i Danmark.

Kommunikation via e-mails anvendes af stort set alle myndigheder, virksomheder og borgere i Danmark. E-mails kan, uden det kræver større teknisk kompetence, misbruges af hackere til at kompromittere en organisation eller person. Det er derfor attraktivt for hackere at gemme falske og skadelige e-mails i strømmen af legitime

e-mails. CFCS vurderer, at de fleste cyberangreb i dag indledes med en phishing-mail.

Det meste phishing er opportunistisk. Det betyder, at alle, som har en mailkonto, kan blive mål for phishing.

Mængden af phishing-mails er så stor, at mange organisationer oplever daglige forsøg på kompromittering via de falske og skadelige e-mails.

Ud over den direkte trussel for en kompromittering svækker phishing også tilliden til e-mails. Det medfører bl.a., at legitime e-mails kan blive forvekslet med phishing.

**Phishing**
Phishing er et forsøg på at narre e-mailmodtagere til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til bl.a. it-systemer.

Ofte vil angriberen ved hjælp af simpel social engineering forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer.

Phishing e-mails sendes ofte bredt ud til mange tilfældige modtagere uden at være tilpasset den enkelte modtager.

**Spear phishing**
Spear phishing er et målrettet forsøg på at narre en eller flere specifikke ofre til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til bl.a. it-systemer. Det foregår eksempelvis via e-mails.

Spear phishing anvender ofte avanceret social engineering for at målrette indholdet til det enkelte offer. Kommunikationen er typisk udformet, så den virker særligt relevant, overbevisende og troværdig for modtageren ved fx at anvende modtagerens navn eller andre oplysninger, som er fundet ved forudgående rekognoscering.

Spear phishing minder om phishing, men adskiller sig især ved, at ofrene ikke er tilfældige, men udvalgte.

Phishing anvendes af mange typer hackere, fra mindre avancerede cyberkriminelle, der arbejder alene, til organiserede kriminelle grupper. I begge tilfælde er målet et økonomisk udbytte. Phishing bruges også i forbindelse med cyberspionage, hvor formålet ofte er at skaffe oplysninger af økonomisk, militær eller politisk betydning.

**Phishing anvendes typisk til et af nedenstående formål:**

- Tyveri af brugernavn og kodeord til internettjenester, som e-mail, sociale medier, webbutikker etc.
- Tyveri af betalingskortoplysninger.
- BEC-svindel, hvor ofret narres til at overføre penge til kriminelle.
- Installation af malware på ofrets computer.
- Få fodfæste i et it-netværk for yderligere kompromittering.
- Tyveri af anden sensitiv eller beskyttelsesværdig information.
- Specielt for Danmark, tyveri af NemID oplysninger.

De oplysninger, en hacker kommer i besiddelse af via phishing, udnyttes af hackeren selv, videresælges eller lækkes til skade for ofret. De kan også videregives til tredjepart, f.eks. i forbindelse med cyberspionage.

De metoder, som anvendes ved phishing, benyttes også i forbindelse med sms'er eller telefonopkald. Her kaldes metoderne henholdsvis smishing og vishing. Et fællestræk ved de tre metoder er, at svagheder i den underliggende teknologi gør det muligt for gerningsmanden at forfalske sin identitet. Af de tre metoder er phishing via e-mails særlig alvorlig for myndigheder og virksomheder. Det skyldes, at medarbejdernes mailklienter befinder sig i it-netværket, hvorfor et phishingangreb kan inficere it-netværket med malware.

**Smishing**
Smishing er phishing forsøg, som foregår via sms. Sms'en vil typisk forsøge at narre modtageren til at gå ind på en hjemmeside for at bekræfte password eller kreditkortoplysninger eller lokke ofret til at downloade en skadelig app. Ofret kan også lokkes til at ringe til et telefonnummer, hvor gerningsmanden vil fortsætte sit svindelnummer.

**Vishing**
Vishing er phishing forsøg via telefonopkald. Gerningsmanden fortæller måske, at ofret har vundet en konkurrence, og skal udlevere personlige oplysninger for at modtage præmien. Gerningsmanden kan også påstå, at ofret har sikkerhedsproblemer med sin computer, betalingskort eller bankkonto og skal udlevere personlige oplysninger eller adgangskoder for at få løst problemet.

**De fleste e-mails er uønskede eller potentielt skadelige**
Danske virksomheder og myndigheder modtager hver dag millioner af e-mails. CFCS vurderer, at op mod 80 procent af de modtagne e-mails er uønskede eller potentielt skadelige. Omfanget af phishing-mails viser, at cyberangreb via phishing udgør en vedvarende trussel.

På grund af omfanget af uønskede og skadelige e-mails anvender de fleste e-mail-tjenester og virksomheder en form for mailfilter. Mailfiltret kigger på forskellige parametre for at afgøre, om en e-mail skal leveres til modtageren, afvises eller sættes i karantæne, indtil modtageren har sagt god for den.

Fordi det kan være vanskeligt med sikkerhed at identificere en phishing-mail, og for ikke at risikere at afvise legitime e-mails, afvises som regel kun e-mails, som filtret vurderer med stor sandsynlighed er uønskede eller skadelige. Det betyder, at et mailfilter ikke vil kunne stoppe alle phishing-mails.

Tests udført at it-sikkerhedsfirmaer har vist, at op til hver tiende phishing-mail slipper igennem et typisk mailfilter.

Den mest almindelige årsag til, at en e-mail afvises, er, at afsender-domænet eller IP-adressen er kendt for at sende uopfordrede reklamer eller phishing. Andre e-mails afvises, fordi de indeholder kendt malware eller links til kendte skadelige hjemmesider. Mere avancerede filtre forsøger at opdage hidtil ukendte phishing-mails og malware. Det sker ved, at filtret leder efter tekst, kodestumper eller handlinger, som indikerer, at indholdet har et skadeligt formål.

**Covid-19 udnyttes i phishing-mails**
Covid-19-pandemien er et godt eksempel på, at cyberkriminelle udnytter borgeres nysgerrighed eller frygt samt efterspørgsel efter viden. Covid-19-pandemien har således været emne i flere phishing-kampagner og falske hjemmesider rettet mod Danmark.

Blandt andet på baggrund af disse phishing-kampagner vedtog Folketinget den 2. april 2020 lovforslaget L 157. Loven giver blandt andet politiet mulighed for at pålægge teleudbydere at blokere adgangen til skadelige hjemmesider med sammenhæng til Covid-19-pandemien. Efterfølgende har CFCS løbende sendt oplysninger om phishing-sider til politiet, hvilket har medført, at der frem til slutningen af september er blokeret mere end 30 phishing-sider målrettet danske borgere.

Hertil kommer, at Center for Cybersikkerhed har identificeret et trecifret antal andre falske hjemmesider, der også forsøger at narre NemID, kreditkort og adgangskoder fra danskerne. Disse sider er forsøgt lukket ved henvendelse til de hostingudbydere, der udlejer serverplads til de kriminelle. Det lykkes ikke altid, og ofte tager det for lang tid i forhold til den kriminelle aktivitet.

CFCS vurderer, at cyberkriminelle fremadrettet også vil forsøge at udnytte statslige kompensationsordninger som tema i phishing-mails.

Øget brug af hjemmearbejde har betydet, at medarbejdere har anvendt nye værktøjer til fjernadgang og samarbejde over internettet. Det

udnyttes også i phishing-kampagner, der forsøger at stjæle adgange til værktøjerne. Fordi medarbejderne ikke er rutinerede i brugen af de nye værktøjer, kan de lettere blive narret af en phishing-mail.

CFCS vurderer, at Covid-19 ikke har medført en generel stigning i cybertruslen mod Danmark. Nogle af de aktører, som allerede anvender phishing, har dog været hurtige til at udnytte pandemien som lokkemad i deres phishing-mails.

DMARC er en teknologi, et stigende antal organisationer anvender. Teknologien kan beskytte en organisations domæner mod at blive misbrugt til phishing. På modtagersiden gør DMARC det muligt for en organisation at afvise e-mails, der er afsendt fra en mailserver, som ikke er knyttet til den organisation, der er angivet som afsender. Det indikerer, at afsenderen ikke er den, vedkommende giver sig ud for, hvorfor der kan være tale om en phishing-mail.

De fleste arbejdsgivere tillader deres medarbejdere at tilgå private mailkonti via virksomhedens computere. De e-mails passerer ikke gennem virksomhedens mailfilter, og virksomheden vælger derfor, mere eller mindre bevidst, at sætte sin lid til, at den pågældende mailtjeneste anvender et mailfilter, og at filtret er effektivt.

En organisation kan få et indtryk af truslen fra phishing ved at undersøge, hvor mange e-mails der afvises af deres mailfilter.

**Hackerne er ofte både dygtige teknikere og menneskekendere**
Før en phishing-mail kan gøre skade, skal den som minimum forbi to forhindringer. Den ene er mailfiltret, og den anden er personen, hvor beslutningen om at klikke på et link eller fil i en e-mail træffes.

Hackerne ved både, hvordan mailfiltre og mennesker reagerer på en e-mail. Der er derfor et konstant kapløb mellem hackerne på den ene side, og på den anden side de sikkerhedsfirmaer, der forsøger at opdage og blokere phishing-mails, samt virksomhederne, der træner medarbejdere i at opdage en phishing-mail.

Nye metoder til at undgå blokering i mailfiltre spredes hurtigt i hackerkredse og via it-sikkerhedsfirmaer, som advarer offentligheden om de nye metoder. Nedenfor er eksempler på metoder, hackere anvender for at snyde et mailfilter.

- Phishing-mails sendes fra konti oprettet ved gratis mailtjenester. Hackeren kan oprette nye konti, hvis de gamle blokeres eller deaktiveres af tjenesteudbyderen.
- Phishing-mails sendes fra legitime, men kompromitterede mailkonti, der ikke er kendt for at sende uønskede eller skadelige e-mails.

- Phishing sendes fra botnet, der er et netværk af computere og andre internetforbundne enheder, som er inficeret med malware, så de kan styres centralt af en hacker. Et botnet skjuler den sande afsender, og sender phishing-mails fra domæner og IP-adresser, der endnu ikke er blokeret af mailfiltret.
- En phishing-hjemmeside flyttes regelmæssigt til et nyt domæne, som endnu ikke er kendt og blokeret af mailfiltret.
- Skadelige filer placeres på en legitim fildelingside, og et link i phishing-mailen henter filen, når modtageren klikker på linket.
- Skadelige filer sløres eller komprimeres, f.eks. i et zip-arkiv, så de ikke umiddelbart kan genkendes eller analyseres af mailfiltret. Mange mailfiltre sætter dog e-mails indeholdende komprimerede filer i karantæne, indtil modtageren har sagt god for e-mailen.
- Phishing-mailen har et link til en kompromitteret men legitim hjemmeside, som videresender besøgende til en skadelig hjemmeside.
- Et skadeligt link indsættes i et vedhæftet dokument, sløres som en QR-kode eller ved hjælp af en tjeneste, som forkorter og ændrer navnet på linket, såsom Bitly.com.
- Teksten i phishing-mailen indsættes som et billede, hvorved teksten typisk ikke kan analyseres af mailfiltret.

**Hackerne kender dig måske bedre, end du tror**

Spear phishing anvendes til målrettede angreb på specifikke personer, grupper eller organisationer, der har hackerens særlige interesse. I stedet for at sende mange enslydende e-mails ud vælger angriberen at tilpasse angrebet til færre specifikke modtagere i håbet om, at en større andel af modtagerne vil åbne mailen. Spear phishing anvendes bl.a. ved BEC-svindel og cyberspionage.

Spear phishing kræver generelt, at afsenderen har et vist kendskab til modtageren. Det kan være personlige eller erhvervsmæssige forhold og interesser. Den viden kan opnås ved at søge information på sociale medier og hjemmesider. Viden om ofret kan i sjældne tilfælde også erhverves mere aggressivt, ved at hackeren, under påskud af sammenfald af interesser eller fagområder, skaber et tillidsforhold til offeret. Kontakten til offeret kan f.eks. ske via sociale medier som LinkedIn og Facebook.

En spear phishing-mail kan indeholde information og links til emner, som målpersonen interesserer sig for fagligt eller privat, men både links og dokumenter kan være falske og skadelige.

Grænsen mellem phishing og spear phishing er flydende. Det, som især adskiller spear phishing fra phishing, er, at ofrene ikke er tilfældige, men nøje udvalgt.

**Sextortion-mails**
Et eksempel på e-mails, der ligner spear phishing, men i realiteten rammer tilfældige ofre, er sextortion-mails. Hackeren har typisk fået adgang til helt tilfældige personers lækkede mailadresser med tilhørende adgangskoder. Hackeren fletter de lækkede adgangskoder ind i enslydende phishing-mails, som sendes til de tilhørende mailadresser.

Hackeren påstår, at have optaget kompromitterende video af modtageren med ofrets webcam. Den lækkede adgangskode skal overbevise modtageren om, at påstanden er sand. Hvis ikke der overføres penge til hackeren, lækkes optagelserne. Medmindre e-mailen indeholder optagelser af modtageren, har hackeren med stor sandsynlighed ikke haft adgang til computeren, og der findes derfor ingen kompromitterende optagelser.

Nogle hackere målretter spear phishing-mails mod medarbejdere med beslutningskompetencer eller ansatte i it-afdelinger. Førstnævnte kan udnyttes i BEC-svindel, og sidstnævnte har ofte administratorrettigheder, så malware let kan installeres på medarbejderens computer. Sidstnævnte kan også have adgang til netværksværktøjer, som angriberen kan udnytte til at trænge længere ind i organisationens it-netværk, når malwaren er installeret på computeren.

**Hackere forsøger at sløre faresignaler i phishing-mails**
Fordi opmærksomheden på phishing generelt er øget i samfundet, afsløres mange banale phishing-mails af årvågne medarbejdere. Som konsekvens er mange hackere blevet mere kreative, og bruger såkaldt social engineering for at få modtageren til at overse eventuelle faresignaler i en phishing-mail.

Social engineering er en angrebsteknik, hvor angriberen anvender psykologiske greb til at opnå offerets tillid, så offeret kan manipuleres til at udføre bestemte handlinger, vedkommende ellers ikke ville have udført. Det kan f.eks. udnyttes til at få ofret til at videregive sensitiv eller klassificeret information uden selv at være klar over det. I phishing-mails udnyttes ofte en persons vanetænkning, autoritetstro, nysgerrighed eller hjælpsomhed.

**Eksempler på social engineering anvendt i phishing-mails**
E-mailen er skrevet på korrekt, eller næsten korrekt, dansk. Det gør modtageren tryg og kan underbygge fornemmelsen af legitimitet.

E-mailen foregiver at komme fra en virksomhed eller myndighed modtageren har tillid til, hvorfor modtageren også har tillid til indholdet i e-mailen. E-mail blev opfundet i en tid, hvor it-sikkerhed endnu ikke var en prioritet. Derfor er det muligt at angive en forfalsket afsenderadresse i en e-mail.

E-mailen indeholder billeder og logoer fra velkendte organisationer, der understøtter afsenderens falske identitet og skaber tillid til indholdet.

Links og vedhæftede filer har navne, som virker tilforladelige, selvom de i virkeligheden fører til en skadelig hjemmeside. Mange brugere er ikke klar over, at navnet på et link ikke behøver at relatere til den hjemmeside, linket fører til.

Indholdet kræver akut handling, og det har påståede negative konsekvenser for modtageren, hvis der ikke tages omgående handling. Håbet er, at ofret ikke bruger den fornødne tid til at vurdere, om e-mailen er ægte.

Indholdet er tillokkende, sensationelt eller skræmmende og vækker stærke følelser, der får ofret til at reagere uovervejet.

Indholdet refererer til et emne, som er meget omtalt i medierne. Håbet er, at modtagerens nysgerrighed vil sløre eventuelle faresignaler og få ofret til at klikke på et vedhæftet link eller dokument.

E-mailen er kort. Overskriften ”Se her” eller ”Kan dette passe?” sammen med et link eller dokument udnytter modtagerens nysgerrighed og indeholder færre elementer, der kan vække mistanke.

**Phishing er en genvej til at installere malware på en computer**
Der er særligt tre metoder, som hyppigt anvendes i forbindelse med kompromittering af en virksomheds it-netværk. Kompromittering af brugernavne og adgangskoder, hacking af virksomhedens internetvendte systemer eller phishing. CFCS vurderer, at phishing er den metode, der anvendes hyppigst. Metoden anvendes både målrettet og opportunistisk.

Ransomware-angreb indledes ofte med en phishingmail. Det var bl.a. tilfældet for det danske firma Danish Agro, som i april 2020 blev ramt af ransomware, hvor det indledende angreb skete via en phishing-mail afsendt fra en kompromitteret underleverandør.

Medmindre hackeren allerede er i besiddelse af et gyldigt brugernavn og kodeord, som giver adgang til virksomhedens it-netværk, er det typisk nemmere at sende malware via et link eller en vedhæftet fil i en phishing-mail end at scanne et it-netværk for åbne porte og hacke sig vej ind i virksomheden via eventuelle sårbarheder i den bagvedliggende software. I sidstnævnte tilfælde kan angrebsfladen være lille og kræve avancerede hackerkompetencer.

Ved phishing er angrebsfladen imidlertid stor. Den svarer til det samlede antal arbejdsrelaterede og private mailkonti, medarbejderne har adgang til fra deres arbejdscomputer. Yderligere passerer phishing-mailen ofte uhindret en perimeter-firewall, som har de porte åbne, der er nødvendige for at sende og modtage e-mails.

Hvis en medarbejder uforvarende åbner en phishing-mail med malware, som er i stand til at udnytte en sårbarhed på medarbejderens computer, vil det, som det var tilfældet med Danish Agro, ofte kun være første trin i cyberangrebet. Den indledende malware kan skabe en bagdør til computeren, som efterfølgende udnyttes af hackeren selv til at downloade yderligere malware og hackerværktøjer, eller adgangen videresælges til andre hackere.

**Statslige hackere anvender også phishing**
Phishing er en effektiv metode til at opnå uautoriseret adgang til en computer eller internettjeneste, og derfor anvendes metoden også af stater, f.eks. i forbindelse med cyberspionage. Brugen af phishing begrænser sig typisk til de indledende faser af et cyberangreb. Først når hackeren har opnået adgang til en computer i det it-netværk, som er mål for cyberangrebet, deployeres de avancerede hackerværktøjer, der giver angriberen en bagdør til it-netværket samt mulighed for at skjule sin tilstedeværelse og bevæge sig videre i it-netværket.

Cyberangreb, herunder phishing-mails, fra statslige aktører vil typisk have til formål at indhente oplysninger af økonomisk, militær eller politisk betydning for landet. Cyberspionage kan ramme alle myndigheder og virksomheder, men er især rettet mod myndigheder og institutioner, der beskæftiger sig med udenrigs- og forsvarspolitik, samfundsvigtige og forskningstunge virksomheder og institutioner samt danske repræsentationer i udlandet.

Statslige aktører har ofte betydelige ressourcer og kan derfor iværksætte phishing-kampagner, der på samme tid er målrettede og foregår i stor skala. Eksempelvis anklagede det amerikanske justitsministerium i 2018 ni iranere, med forbindelse til den iranske stat, for at stå bag spear phishing-angreb mod 320 universiteter i 21 lande, herunder Danmark.

Ifølge anklagen sendte iranerne i perioden 2013 til 2017 mere end 100.000 spear phishing-mails til professorer verden over. Indholdet refererede til artikler skrevet af modtageren og indeholdt links til hjemmesider med relation til modtagerens forskning. I virkeligheden førte et af de vedhæftede links til en falsk login-side, som lignede den, der blev anvendt af universitetet. Herved

kunne hackerne stjæle loginoplysninger og selv få adgang til det aktuelle universitet.

DKCERT, som overvåger sikkerheden på forskningsnettet, opdagede tilbage i januar 2015 et phishingangreb, som med meget høj sandsynlighed var en del af ovenstående phishing-kampagne. Ifølge DKCERT førte angrebet til, at 25 medarbejdere på danske universiteter fik kompromitteret deres adgangskoder.

**Phishing-mails kan komme fra en samarbejdspartner**
CFCS har kendskab til flere tilfælde, hvor kompromitterede mailkonti er anvendt til at sende phishing-mails til kontakter i andre danske virksomheder.

Det er svært for modtageren at afsløre svindlen, da phishing-mailen ser ud til at komme fra en person eller virksomhed, modtageren kender og har tillid til. Angrebet kan på den måde sprede sig fra en kompromitteret mailkonto i en virksomhed til en mailkonto i en anden virksomhed, hvor angrebet kan fortsætte.

Hvis de cyberkriminelle får adgang til en mailkonto, der anvendes til fakturering, kan de sende nye falske fakturaer med de kriminelles kontonummer, eller ændre kontonummeret i en eksisterende faktura. Særligt hvis den falske e-mail sættes ind i en eksisterende mailkorrespondance, vil modtageren have svært ved at afsløre svindlen uden at tjekke det opgivne kontonummer. En metode til at imødegå den type svindel er, at man ved enhver udbetaling sikrer, at kontonummeret er korrekt, uanset om der er tale om en dansk eller udenlandsk bank.

Udsendelse af phishing-mails, som lægger sig i en eksisterende mailkorrespondance, kræver normalt at hackerne udformer de falske e-mails manuelt. I 2019 begyndte organiserede kriminelle imidlertid at anvende automatiserede systemer til at udsende malware i tusindvis af phishing-mails, som foregav at være et svar på en eksisterende mailkorrespondance. Indholdet og modtageradresserne i de falske e-mails var stjålet ved en tidligere kompromittering.

**Cyberkriminelle fisker efter logins til virksomheders cloudmail**
Mere end halvdelen af alle større danske virksomheder benytter kontorværktøjer og e-mail, der leveres som en cloudløsning. CFCS vurderer, at virksomheders cloudmail er udsat for en vedholdende cybertrussel, og bl.a. er et populært mål for phishing.

CFCS har kendskab til flere tilfælde, hvor danske virksomheders cloudløsning er forsøgt kompromitteret ved hjælp af phishing. Cyberkriminelle sender phishing-mails til medarbejdere indeholdende et link til en falsk login-side til virksomhedens cloudløsning.

Hvis en medarbejder indtaster brugernavn og adgangskode på den falske hjemmeside, får de kriminelle adgang til medarbejderens mailkonto, og kan

f.eks. anvende den til yderligere phishing internt i virksomheden eller mod kunder og underleverandører.

Den bedste beskyttelse mod den type svindel er multi-faktor autentifikation (MFA). Det gør det vanskeligere, men ikke umuligt at udføre svindlen.
En af metoderne, hackerne bruger til at omgå MFA, er at overføre ofrets brugernavn og adgangskode fra den falske hjemmeside til den ægte. Når MFA-koden derefter bliver sendt til ofret, og ofret skriver koden på den falske login-side, benytter hackeren koden på den ægte hjemmeside, og har dermed adgang. For at ofret ikke skal få mistanke, sender hackeren en fejlbesked til ofret om, at login ikke lykkedes. Metoden er vanskelig, fordi den skal udføres, inden MFA-koden udløber. Samtidig giver metoden kun adgang til kontoen en gang.

Microsoft oplyser, at 99,9 % af virksomhederne, der får kompromitteret deres Office365 løsning, ikke har anvendt MFA, og at det globalt set kun er 11 % af virksomhederne, som har aktiveret MFA. CFCS vurderer, at der også i Danmark er mange virksomheder og private e-mail-brugere, der stadig ikke har implementeret MFA-login.

**Det meste phishing har forbindelse til organiseret kriminalitet**
Cyberkriminelle behøver ikke selv at opbygge en phishing-kampagne fra bunden. I stedet er det muligt for hackere at skaffe alt det, som er nødvendigt, via et undergrundsmarked der er skabt og drevet af organiserede kriminelle, der sælger eller lejer deres værktøjer og infrastruktur til andre, som ønsker at lave phishing.

Tjenesterne kan typisk betales anonymt med kryptovaluta, og hvis hackerne har succes med deres phishing, kan de stjålne data og adgange sælges videre til andre kriminelle.

Mailadresser til ofre samt malware kan således købes på internettet, og distributionen af phishing-mails kan ske fra et botnet drevet af andre hackere. Phishing-hjemmesider kan let oprettes ved hjælp af phishing kits, og virksomheder, der udbyder såkaldt bulletproof hosting, gør det muligt for hackere at oprette og drive phishing-hjemmesider på en måde, der gør det svært for myndighederne at gribe ind.

Myndigheder i flere lande forsøger at lukke sådanne udbydere. I september 2019 lukkede tysk politi en hostingudbyder, som opererede fra en tidligere NATO-bunker. Bunkeren indeholdt 200 servere med bl.a. ulovlige hjemmesider. Måneden efter blev den hollandske hosting-udbyder KV Solutions lukket. Udbyderen havde bl.a. tilladt kriminelle at oprette falske hjemmesider på dens servere.

Udover at drive en kriminel forsyningskæde, der understøtter udsendelse af phishing-mails, står de organiserede kriminelle grupper også for en stor del af de phishing-mails, der sendes ud.

**Phishing kit**
Det er ikke trivielt at lave en falsk hjemmeside, som ligner og fungerer som en ægte webshop eller login-side. Cyberkriminelle, som ikke selv har evnerne, kan særlige steder på internettet købe såkaldte phishing kits, der indeholder alle de værktøjer og services, som skal til for at oprette og drive en falsk hjemmeside.

Kriminelle uden hackerkompetencer kan endda købe såkaldt phishing-as-a-service på internettet. Her driver udbyderen den nødvendige infrastruktur, der kræves for at lave phishing.

**Bulletproof hosting**
Bulletproof hosting betegner en hostingudbyder, som tillader kriminelle at leje deres servere for at anvende den til cyberkriminalitet. De reagerer typisk ikke på henvendelser fra myndigheder eller virksomheder, der er blevet svindlet, hvorfor det kan tage lang tid at lukke en phishing-hjemmeside.

Emotet er et eksempel på et berygtet botnet, som drives af organiserede kriminelle. I 2019 bestod botnettet af mere end 120.000 inficerede internetforbundne enheder. Efter et fald i aktiviteten over sommeren 2019, som ifølge sikkerhedsfirmaer medførte et globalt fald i antallet af registrerede phishing-mails på næsten 40%, steg aktiviteten igen, og der blev i oktober og november samlet registreret næsten 11 millioner phishing-mails fra netværket.

Rapporter fra sikkerhedsfirmer, som sporer enheder, der indgår i botnet, viser, at der også i danske it-netværk er et stort antal computere og andet internetforbundet udstyr, der indgår i botnet. Nogle danske teleudbydere arbejder aktivt på at opspore og få renset disse enheder hos deres kunder, hvilket medvirker til at mindske truslen fra phishing og anden cyberkriminalitet.

**Fungerende mailadresser er eftertragtede af cyberkriminelle**
Phishing kræver adgang til fungerende mailadresser. Derfor er mailadresser, ligesom adgangskoder, eftertragtede af hackerne.

Mange legitime virksomheder på internettet sælger lister med mailadresser. De giver ofte køberen mulighed for at vælge land, sektor, virksomhed eller om det skal være mailadresser til ledende medarbejdere. Maillisterne anvendes typisk i forbindelse med markedsføring, men kan også misbruges til phishing. Der findes også tjenester som eksempelvis hunter.io, hvor det er muligt at søge i en database med indsamlede mailadresser. Der kan f.eks. søges på mailadresser tilhørende en specifik virksomhed.

Mange mailadresser indsamles med software, som afsøger hjemmesider, internetforums og sociale medier for mailadresser. Vil hackeren selv samle mailadresser, kan softwaren let købes og downloades fra internettet. Det

betyder, at mailadresser som er eksponeret på internettet, kan være særlig udsat for phishing og andre uønskede e-mails.

Mailadresser kan også stamme fra virksomheder og hjemmesider, der tilbyder et produkt eller en service gratis, f.eks. nyhedsbreve, rapporter og lignende, mod at modtageren oplyser sin e-mailadresse.

Hackere høster ofte mailadresser fra de borgere, virksomheder eller internet-tjenester, de har kompromitteret. Der kan være tale om kontaktlister eller kundedata. Mailadresserne bliver enten solgt, eller hackeren bruger dem selv i andre hackerangreb. Filer med kompromitterede mailadresser bliver nogle gange lækket på internettet, hvor hackere kan samle dem op og misbruge dem.

Mængden af lækkede mailadresser er enorm. Hjemmesiden haveibeenpwned.com indeholder næsten 10 milliarder e-mailadresser, som stammer fra datalæk. På siden kan privatpersoner, virksomheder og myndigheder undersøge, om deres mailadresser er blevet eksponeret i et datalæk. Det er også muligt at se, hvilken virksomhed eller internettjeneste datalækket stammer fra.

Ved spear phishing er hackeren villig til at bruge lang tid på at finde e-mailadressen til ofret. Oplysningerne kan måske findes på virksomhedens hjemmeside, eller spear phishing bliver sendt til organisationens hoved e-mailadresse i håb om, det giver adgang til målpersonen.

Hackeren kan også gætte mailadressen. Virksomheders mailadresser anvender ofte en fastlagt syntaks, som kan ses, blot hackeren har kendskab til en tilfældig medarbejders navn og mailadresse, f.eks. via virksomhedens hjemmeside. Herefter er det relativt enkelt at gætte mailadressen til en specifik medarbejder, som kan være fundet via Linkedin. Da mailsystemer typisk sender en fejlmeddelelse til afsenderen, hvis modtageren ikke eksisterer, er det let for hackeren at vide, hvornår modtageradressen er korrekt.

Ovenstående metode kan også anvendes til at finde flere valide mailadresser i en specifik virksomhed blot ved at prøve sig frem med forskellige mailadresser for det pågældende maildomæne.

**Tusindvis af nye phishing-hjemmesider åbner hver dag**

I 2019 detekterede organisationen Anti-Phishing Working Group (APWG) gennemsnitligt 65.000 nye phishing-hjemmesider hver måned. Mange af de falske hjemmesider er oprettet ved hjælp af såkaldte phishing kits, som der hvert år detekteres hundredvis nye af. Eksempelvis har et phishing kit målrettet Office365 været anvendt mod danske virksomheder.

De mange nye phishing-sider betyder, at der altid vil være nye falske hjemmesider, som mailfiltre og andre sikkerhedssystemer endnu ikke kender og blokerer.

**De mange nye topdomæner udnyttes til phishing**
Phishing-hjemmesider forsøger ofte at narre besøgende ved at have et navn, der kan forveksles med navnet på en legitim hjemmesideside. Fordi der i dag findes mere end 1500 såkaldte topdomæner, der populært sagt er hjemmesidens efternavn, kan navnet på den falske hjemmeside være identisk med den ægte side, men blot ligge på et andet topdomæne, f.eks. xyz i stedet for dk. Under Covid-19-pandemien har CFCS f.eks. medvirket til at fjerne phishing-hjemmesiden sundhedsstyrelsen.net, der efterlignede hjemmesiden sundhedsstyrelsen.dk.

Enkelte mindre lande som Gabon i Afrika og Tokelau, der er en øgruppe under New Zealand, tilbyder gratis domæner på deres topdomæner .ga og .tk. Det udnyttes af nogle cyberkriminelle til at anskaffe gratis domæner til deres falske hjemmesider.

**Fjernelse af falske hjemmesider kan gøre en phishing-mail harmløs**
De fleste phishing-mails fungerer i samspil med en falsk og skadelig hjemmeside. Uden hjemmesiden bliver den slags phishing-mails harmløse. Derfor er fjernelse af phishing-sider vigtig for imødegåelse af truslen.

Myndigheder og sikkerhedsfirmaer arbejder hele tiden på at opdage og lukke eller blokere phishing-hjemmesider. Som modtræk skifter de kriminelle f.eks. løbende navn på de falske hjemmesider, flytter dem til servere med nye IP-adresser eller obfuskerer den kode, som skaber den falske hjemmeside. Et andet modtræk er, at nogle phishing-sider kun er tilgængelige få timer eller dage, når phishing-kampagnen kører. En phishing-side kan derfor være åben i få timer for derefter at lukke, blot for at genopstå igen efter nogle dage.

Hackere kan også sløre eksistensen af en phishing-hjemmeside ved at blokere adgangen til siden fra IP-adresser og domæner, der f.eks. tilhører sikkerhedsfirmaer, netværksscannere og søgemaskiner.

Når en phishing-side kun eksisterer i kort tid, skifter navn eller IP-adresse eller på anden måde skjules for myndigheder og sikkerhedsfirmaer, er det vanskeligt at opdage og efterfølgende lukke eller blokere hjemmesiden.

**Mange medarbejdere kan blive snydt af en phishing-mail**
Risikoen for at en medarbejder lader sig narre af en phishing-mail afhænger både af, hvor godt e-mailen er udformet, og hvilken træning medarbejderen har modtaget i at opdage forsøg på phishing. For at beskytte myndigheden eller virksomheden er det derfor vigtigt at inddrage medarbejderne som en del af forsvaret mod phishing-mails.

Test udført af it-sikkerhedsfirmaer viser, at cirka 30 procent af medarbejdere, som ikke har fået træning, klikker på et link i en phishing-mail, og at tallet falder til omkring 10 procent, når medarbejderne har modtaget træning. Ved tilbagevendende træning kan tallet komme endnu længere ned, men det vil aldrig blive nul.

Cirka 70 procent klikker på et link i en spear phishing-mail, og hvis mailen er modtaget fra en intern mailkonto, vil de fleste medarbejdere opfatte e-mailen som ægte.

**Et godt cyberforsvar kan imødegå følgerne af phishing**
En virksomheds it-sikkerhed afhænger som regel af de beslutninger og tiltag, sikkerhedseksperter i it-afdelingen foretager. Når en phishing-mail ender i en medarbejders mailboks, er virksomhedens it-sikkerhed imidlertid delvist ude af sikkerhedseksperternes hænder og afhænger af, om medarbejderen uforvarende åbner phishing-mailen.

Fordi mailfiltre og træning af medarbejdere ikke kan stoppe alle phishing-mails hver eneste dag, er det vigtigt, at virksomhedens øvrige cyberforsvar kan imødegå eventuelle følger af et succesfuldt phishing-angreb.

Eksempelvis kan en "sikker DNS-tjeneste" blokere adgangen til kendte skadelige hjemmesider, MFA kan gøre det vanskeligt at udnytte stjålne brugernavne og adgangskoder og application whitelisting kan forhindre installation af skadelig software fra vedhæftede filer og hjemmesider.

Hvis skadelig software som malware alligevel bliver installeret, kan antivirus og antimalware-systemer opdage og fjerne malwaren. Endelig kan gode administrative procedurer forhindre, at penge udbetales til svindlere som følge af en phishing-mail.

Hvis skaden er sket, så er det tiltag som logning, backup og effektive beredskabsplaner, der vil medvirke til at mindske konsekvensen for organisationen.

**Anbefalinger**
CFCS anbefaler alle myndigheder og virksomheder at orientere sig om truslen fra phishing og inddrage truslen i deres risikovurdering.

På siden cfcs.dk findes følgende relevante vejledninger:

- Phishing – beskyt din organisation mod phishingangreb
- Reducér risikoen for falske e-mails
- Passwordvejledning
- Cyberforsvar der virker

**Trusselsniveauerne**

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

| | |
|---|---|
| **INGEN** | Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig. |
| **LAV** | Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig. |
| **MIDDEL** | Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig. |
| **HØJ** | Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig. |
| **MEGET HØJ** | Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig. |

FE bruger denne skala for sandsynligheder i analyser