CENTER FOR CYBERSIKKERHED

Vejledning

Phishing

Beskyt organisationen mod phishing-mails.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

3. udgave oktober 2022.
Forsideillustration: simarik/iStockPhotos

Indledning

Phishing udgør en vedvarende og alvorlig trussel mod alle myndigheder, virksomheder og borgere i Danmark. Mængden af phishing-mails er så stor, at mange organisationer oplever daglige forsøg på kompromittering.

Det er svært at opdage, om en mail er et phishing-angreb. Hvis det er et spear phishing-angreb, kan det være endnu sværere. Det er derfor vigtigt, at organisationen benytter sig af forskellige tiltag til at beskytte sig imod phishing-angreb. Vejledningen omhandler både phishing og spear phishing, da de beskrevne tiltag vil bidrage til at beskytte mod begge typer angreb.

Læsevejledning
I denne vejledning fokuseres på phishing gennem mails. Men phishing kan også ske via SMS (smishing), telefonopkald (vishing), chatapplikationer og sociale medier.

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.

Vejledningen henvender sig til organisationens ledelse. Det er hensigten, at vejledningen kan indgå i organisationens arbejde med at forhindre, at truslen fra phishing-angreb udsætter organisationen for unødigt store risici.

Vejledningen er inddelt i fem afsnit, der hver især indeholder anbefalinger til, hvad der kan hjælpe organisationen med at reducere risikoen fra phishing:

Phishing. Afsnittet beskriver, hvad phishing er, og hvordan metoden adskiller sig fra spear phishing. Dernæst forklares, hvad phishing bliver brugt til, og en række phishing karakteristika beskrives.

Gør det svært at lykkes med phishing. Afsnittet er inddelt i to underafsnit. Ét, der beskriver sikringstiltag målrettet modtagelse af mails og ét, der beskriver tiltag målrettet udsendelse af mails. Både tekniske og organisatoriske tiltag beskrives.

Opdag tegn på phishing. Dette afsnit beskriver karakteristika ved phishing, der kan hjælpe organisationen til at opdage mails modtaget fra ondsindet aktør.

Begræns konsekvenserne af ikke opdagede phishing-angreb. Afsnittet gennemgår en række foranstaltninger, der bidrager til at begrænse de potentielle konsekvenser et vellykket phishing-angreb kan have for organisationen.

Håndter phishing-angreb. Vejledningens afsluttende afsnit beskriver nødvendigheden af at have tilstrækkelig logning samt planer og processer på plads for at kunne håndtere en sikkerhedshændelse, når den sker.

Overordnede anbefalinger

Nedenfor opstilles Center for Cybersikkerheds overordnede anbefalinger til hvordan organisationen kan reducere risikoen fra phishing-angreb. Anbefalingerne uddybes i de følgende afsnit.

Anbefalingerne i denne vejledning er et udvalg og skal ikke opfattes som en udtømmende liste.

- Udarbejd processer, der kan bidrage til at reducere risikoen fra phishing-angreb. Det kan eksempelvis være processer for pengeoverførsler, for indrapportering om mulige phishing-mails, for brug af sociale medier og for brug af mail.
- Behandl indkommende mails i henhold til afsenderdomænets DMARC-politik.
- Installer antivirus, brug mailfiltre og sørg for at de er løbende opdateret.
- Undgå at mails indeholder links til websider, hvorfra der er direkte login med NemID eller andre loginløsninger.
- Minimer mængden af tilgængelig information om organisationen og medarbejderne.
- Hvis der er mistanke til en mails ægthed, kontakt afsenderen på anden vis for at få bekræftet afsenderens identitet og ægtheden af mailen.
- Gør det nemt at rapportere om mulige phishing-mails.
- Introducer medarbejderne til organisationens kommunikationspolitik, undgå phishinglignende kommunikation i både – intern og ekstern kommunikation.
- Anvend DMARC med en REJECT-politik, og implementerer SPF og DKIM på alle organisationens domæner.
- Hold systemer, programmer og enheder opdateret.
- Anvend application control løsninger, der sikrer, at kun autoriserede programmer aktiveres på enheden.
- Implementer tiltag som sikker DNS, der beskytter brugerne mod kendte ondsindede hjemmesider.
- Anvend flerfaktor-autentifikation. Det gør det sværere for hackere at få adgang til systemer eller konti, hvor en medarbejder er blevet narret til at afgive loginoplysningerne.
- Hav politik for logning, som sikrer at gode og anvendelige logs er tilgængelige.
- Hav planer for hændelseshåndtering og beredskab, og test dem regelmæssigt.

Phishing

Phishing er forsøg på via social engineering at manipulere en person til i god tro at:

- videregive personlige oplysninger,
- klikke på inficerede filer eller links til falske hjemmesider,
- give uretmæssig adgang til blandt andet it-systemer, eller til at
- udføre kommandoer på egen PC.

Phishing-mails sendes ofte bredt ud til mange modtagere.

Et spear phishing-angreb er målrettet enkeltpersoner i en organisation. Formålet kan være at hente fortrolige forretningsoplysninger, bruger-id og adgangskoder til konti med mere ud af en organisation. Et typisk spear phishing-angreb udsendes ofte kun til få udvalgte personer. For angriberen vil det normalt kræve en vis research for at sikre, at den fremsendte mail virker relevant, overbevisende og tillidsvækkende.

Social engineering

Social engineering er en teknik, hvor der anvendes psykologiske greb til at få offeret til, i god tro, at udføre en handling, vedkommende ellers ikke ville have udført. Det kan eksempelvis være at afgive loginoplysninger eller videregive informationer om organisationen, dens processer, systemer eller kunder.

Social engineering kræver et vist kendskab til offeret for at være effektiv. Derfor bliver der ofte anvendt information om ofret eller arbejdspladsen, som er fundet på hjemmesider eller sociale medier ved forudgående rekognoscering.

En spear phishing mail er typisk karakteriseret ved, at:

- Den indeholder informationer, som kun få personer burde kende til. Dette kan for eksempel være om specifikke arbejdsopgaver, personlige relationer eller forhold, herunder private interesser og økonomiske forhold.
- Oplysningerne kan være hentet fra sociale medier som Facebook eller LinkedIn eller virksomhedens hjemmeside.
- Mailen er udformet således, at den tilsyneladende kommer fra en troværdig afsender i modtagerens egen organisation eller fra en kendt, troværdig samarbejdspartner.
- Sproget i mailen er godt formuleret.
- Der optræder ikke trusler eller anden opfordring til presserende handlinger.

Hvad bruges phishing til?
Phishing bruges typisk til at:

- Fremskaffe brugernavn og password til internettjenester. Det kan være til mailkonto, sociale medier, webbutikker.
- Fremskaffe anden sensitiv eller beskyttelsesværdig information, for eksempel, om virksomhedens it-systemer, adgang til wifi.
- Fremskaffe betalingskortoplysninger.
- Fremskaffe NemID oplysninger.
- Ofret narres til at overføre penge til kriminelle, for eksempel til direktørsvindel.
- Installere malware på ofrets enhed.
- Få fodfæste i et it-netværk for yderligere hacking.

Business Email Compromise (BEC) / direktørsvindel

BEC-svindel, også kendt som direktørsvindel (CEO-fraud), er forsøg på at franarre virksomheder og organisationer penge gennem falske anmodninger om pengeoverførelser. I stedet for at sende mails til en stor gruppe tilfældige medarbejdere i en virksomhed, laver hackerne grundig research. Det gør dem i stand til at lave troværdige, målrettede mails, hvor de f.eks. udgiver sig for at være en direktør, økonomichef eller konsulent i tæt kontakt med den øverste ledelse og derved lokke ansatte til at agere i den tro, at det er efter ordre fra ledelsen. Dette kan blive kombineret med et beskrevet tidspres på ordren. Der får det til at se ud som om der skal ageres hurtigt.

De bedrageriske mails sendes ofte fra fremmede mailkonti. Men i nogle tilfælde misbruges kompromitterede mailkonti, der tilhører ledende medarbejdere i virksomheden. Fremsendelse af falske mails fra sådanne kompromitterede konti kan øge risikoen for at bedrageriforsøg lykkes.

Opdag tegn på phishing

Selvom det kan være svært at opdage phishing-mails, så har de en række kendetegn.

- Mange phishing-angreb forsøger at udnytte følelser som nysgerrighed, bekymringer og et ønske om at ville hjælpe. Det gør hackerne, fordi de ved, at hvis vi handler følelsesmæssigt, så kan det påvirke vores beslutningsevne i øjeblikket. Det kaldes også for social engineering.
- Hackerne bruger et emne, som er oppe i tiden og får meget medieomtale. Eksempelvis når Skat frigiver årsopgørelserne eller når det er Black Friday.
- Modtageren opfordres til at gøre noget, der ikke følger organisationens normale processer. Og det skal gøres nu. Det gør hackeren i håb om, at modtageren handler følelsesmæssigt og ikke bruger ekstra tid til at vurdere, om mailen er ægte.
- Mailen afviger fra normalen. Det kan eksempelvis være, hvis afsenderen kontakter modtageren gennem et medie, organisationen ikke normalt bruger. Eller hvis kontekst eller ordvalg afviger fra det forventede og kendte. Der er ofte tale om små afvigelser, der kan være svære at forklare som andet end en mavefornemmelse.
- Vær opmærksom på URL'er i mailen. Hackere anvender domænenavne, der ved første øjekast ser legitime ud, for eksempel Linkdin.com i stedet for LinkedIn.com. Er man i tvivl, bør man selv skrive URL'en til det ønskede domæne ind i browseren, uden at interagere med hyperlinket i mailen.

Gør det svært at lykkes med phishing-mails

Organisationen bør implementere både organisatoriske og tekniske sikringstiltag for at forhindre phishing-forsøg i at lykkes. Begge former for sikringstiltag bliver beskrevet i det følgende. Først med fokus på modtagelse af mails, derefter med fokus på udsendelse af mails.

Når der modtages mails

Installer antivirus og brug mailfiltre
Ved at installere antivirus og bruge mailfiltre, kan man filtrere eller blokere for uønskede mails, inden de når frem til brugernes indbakke. Konkret opnås effekten ved at lade antivirus og mailfiltre tjekke alle de mails, organisationen modtager, for tegn på spam, phishing eller malware.

Forskellen mellem filtrering og blokering er, at en mail, der fanges af et mailfilter sædvanligvis flyttes til en anden mappe end indbakken, mens en mail, der blokeres, aldrig når frem til brugeren.

Reglerne for henholdsvis filtrering og blokering bør tilpasses de konkrete forhold i organisationen. Der kan være behov for at tilpasse de opsatte regler i takt med at organisationen, trusselsbilledet og tendenserne ændrer sig.

Organisationen bør udarbejde klare retningslinjer og fastlægge processer for håndtering af medarbejdernes mails. Det bør sikres, at medarbejderne er blevet gjort bekendt med retningslinjerne.

Mails kan filtreres eller blokeres på forskellige måder. Eksempelvis ud fra IP-adresse, afsender-domænenavn, omdømme, indhold, afsenderens DMARC-politik, og filtype for vedhæftede filer.

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

Behandl indkommende mails i henhold til afsenderdomænets DMARC-politik

Når der modtages mails, bør afsenderens DMARC-, SPF- og DKIM-politikker respekteres.

Ved at validere DMARC-politikken på indkommende mails kan visse forfalskede mails opdages, inden de leveres til modtagere i organisationen.

Sender Policy Framework (SPF)
SPF-mailgodkendelsesmetoden (Sender Policy Framework) sigter mod at reducere spam og svindel ved at gøre det vanskeligere for mailafsendere at skjule deres identitet. SPF registrerer mailspoofing ved at levere en proces til at bekræfte, hvem der har tilladelse til at sende mails på dine vegne.

DomainKeys Identified Mail (DKIM)
DKIM er domæneejeres mulighed for kryptografisk at signere afsendte mails på vegne af domænet, de er sendt fra. Det fungerer ved at signere hver enkelt mail med en privat nøgle, så den modtagende mailserver kan bekræfte, at den kommer fra det angivne domæne ved at verificere signaturen med den tilhørende offentlige nøgle.

Domain-based Message Authentication, Reporting and Conformance (DMARC)
DMARC (Domain-based Message Authentication, Reporting, and Conformance) er en mailgodkendelse, politik og en rapporteringsprotokol. Den er oprettet oven på SPF-(Sender Policy Framework) og DKIM-(DomainKeys Identified Mail) protokoller. Hvis ingen af disse godkendelsesmetoder bestås, bestemmer DMARC-politikken, hvad der skal gøres med meddelelsen.

Ved tvivl få afsenders identitet bekræftet
Organisationen skal sikre, at medarbejderne ved, at hvis der er mistanke om, at en afsender ikke er den, han eller hun giver sig ud for at være, så skal medarbejderen lade være med at svare i samme tråd. Eksempelvis ved at skrive en ny mail og sende den til den e-mailadresse, medarbejderen har til vedkommende. På den måde startes en ny mailtråd, så den gamle ikke fortsættes.

Medarbejderen kan også ringe til afsenderen. Her bør det telefonnummer, medarbejderen har på vedkommende, anvendes i stedet for et telefonnummer, der fremgår af mailen. Alternativt kan medarbejderen ringe til det telefonnummer, som oplyses på den pågældende organisations officielle hjemmeside.

Gør det nemt at rapportere om mulige phishing mails
En velfungerende indrapporteringsproces sikrer at I har vigtig information om hvilke typer phishing-angreb der bliver brugt mod jeres organisation. Samtidig giver den mulighed for at se hvilke typer mails, der fejlagtigt opfattes som forsøg på phishing i organisationen.

For at have en velfungerende indrapporteringsproces, skal brugerne føle sig trygge. Så trygge, at de tør fortælle om de tilfælde, hvor de har klikket på et link eller åbnet en vedhæftet fil, og efterfølgende har en fornemmelse af, at det var en fejl.

Derfor er det vigtigt, at der er afsat ressourcer til at håndtere indrapporteringerne, så brugerne modtager hurtig feedback. Det kan være med en besked om, hvad der er sket på baggrund af deres indrapportering. Og en besked som gør det klart, at hver enkelt rapportering gør en forskel – også i de tilfælde hvor der ikke er tale om en phishing-mail.

Indrapportering kan eksempelvis ske til it-afdelingens servicedesk, der bør kunne vejlede om phishing mails og undersøge, om der er tale om et forsøg på phishing eller ej.

Minimer mængden af tilgængelig information om organisationen
For at gøre phishing-mails mere overbevisende undersøger hackere blandt andet hvilke oplysninger der ligger frit tilgængeligt på internettet om den pågældende organisation. Som organisation kan I med fordel gøre jer en række overvejelser:

- Hvilke oplysninger er nødvendige for besøgende på jeres hjemmeside?
- Hvilken detaljegrad bør oplysningerne have?
- Har I et overblik over, hvilke oplysninger der er på internettet om organisationen og jeres medarbejdere? Eksempelvis kontaktoplysninger på medarbejdere og ledelsen.
- Har I et overblik over, hvilke oplysninger jeres leverandører, samarbejdspartnere og kunder deler om organisationen?
- Har I en politik for hvad medarbejderne må skrive om organisationen på deres sociale medier? Hvis ikke - har I så brug for en?
- Skal medarbejdere, hvis mailadresser er tilgængelige på internettet, modtage særlig træning om phishing?

Hvis I ved hvilken information, der er tilgængelig på internettet om organisationen, er det nemmere for jer at vide, hvilken information hackerne kan bruge mod jer i et spear phishing-angreb.

Hav processer og kend dem
I arbejdet med at reducere risikoen for vellykkede phishing-angreb, er det vigtigt at medarbejdere og brugere/kunder kender de vedtagne processer for jeres arbejdsgange.

Det kan være processen for pengeoverførsler eller for hvordan særlige typer af information deles. På den måde har medarbejderne et bedre grundlag for at spotte usædvanlige forespørgsler, der kan være et forsøg på eksempelvis direktørsvindel.

I kan også have specifikke processer for hvordan mails håndteres. Eksempelvis at alle forespørgsler af en specifik type skal bekræftes gennem en anden kommunikationsform. Eller at særlige filer kun deles gennem en sikker fildelingstjeneste, frem for at filerne deles som vedhæftninger i mails.

I bør også overveje, om visse processer bør følge princippet om funktionsadskillelse. Det vil sige, at en aktivitet ikke kan gennemføres af en enkelt person eller gruppe. Eksempelvis at skift af en leverandørs betalingsoplysninger skal bekræftes af én medarbejder og godkendes af en anden.

I bør udarbejde en proces for anmeldelse og håndtering af phishing-mails, herunder hvordan hændelser forsaget af phishing-mails håndteres.
Denne proces bør også omfatte varsling af ansatte under særlige omstændigheder, eksempelvis når organisationen er ramt af omfattende phishing eller spear phishing angreb.

Processerne bør være forankret i den overordnede informationssikkerhedspolitik og de tilhørende målsætninger for informationssikkerhed. Det bør også klart fremgå, hvem i organisationen har ansvaret for at iværksætte, øve og lede dem.

Når der udsendes mails

Anvend DMARC, SPF og DKIM, og bekæmp spoofing

DMARC kan forhindre, at en anden kan udsende falske mails, der ser ud til at komme fra jeres organisation. Det bliver også kaldt spoofing.

Hvis DMARC implementeres på jeres domæne, og en ondsindet aktør forsøger at sende en mail med jeres domæne som afsender, vil modtagerens mailserver kunne bruge DMARC oplysningerne til at afvise mailen. På den måde beskyttes slutbrugeren mod mails med en falsk afsenderadresse.

Desuden indeholder DMARC en rapporteringsfunktion, der gør det muligt for en domæneejer at modtage rapporter over andres forsøg på at sende forfalskede mails på vegne af domænet. Uden brug af DMARC vil ejeren af et misbrugt domæne ikke blive informeret om misbruget.

Der er en række fordele ved at bruge DMARC, og gevinsterne ved at bruge DMARC stiger i takt med, at flere organisationer anvender teknologien, hvilket kommer hele samfundet til gavn:

- Afsenders omdømme beskyttes ved at gøre det sværere at udsende falske e-mails. På den måde vil organisationens navn ikke blive synonymt med forsøg på svindel.
- Organisationens kunder og samarbejdspartnere får garanti for afsender-autenticiteten i de mails, der er udsendt med organisationens domæne som afsender.
- Bidrager til at give et overblik over misbrug af organisationens domæner.

For at DMARC kan beskytte et domæne, kræver det, at SPF og/eller DKIM implementeres. Selvom brugen af DMARC, SPF og DKIM er gode værn mod spoofing, giver de ikke beskyttelse mod andre typer misbrug, som for eksempel typosquatting, hvor et falsk domænenavn er designet specifikt til at kunne forveksles med et legitimt domænenavn.

Alle statslige myndigheder er forpligtet til at sikre deres domæner med en DMARC REJECT-politik.

Undgå at bruge phishing-lignende kommunikation

For at kunne genkende et phishing-forsøg, kræver det at man kender den form for kommunikation organisationen bruger.

Som organisation skal I, via jeres kommunikationspolitik, give retningslinjer for intern og ekstern kommunikation, og arbejde på at eliminere eventuel phishing-lignende kommunikation. Det gælder både jeres interne og eksterne kommunikation.

I den interne kommunikation kan I eksempelvis arbejde hen imod at undgå mails til kollegaen med emnefeltet ”Haster: kommentarer til vedhæftede”.

I bør også overveje jeres egen brug af links i mails og om mængden af links kan minimeres.

Mails bør ikke indeholde links til websider, hvorfra der er direkte login med NemID eller andre loginløsninger.

I kan eksempelvis referere til jeres egen hjemmeside blot med navn eller til hjemmesiden uden link og præfiks (www. eller https://).

Hvis I vurderer, at det er nødvendigt at dele links via mails, så bør det tilstræbes at gøre jeres links gennemskuelige for eksterne modtagere. Det kan især være relevant i de tilfælde, hvor der anvendes en leverandør til udsendelse af nyhedsbreve. Gennemskueligheden kan eksempelvis opnås ved at link og afsenderdomæne er det samme.

Derudover kan I opfordre til, at mails ikke anvendes til deling af filer og links, men at disse i stedet deles internt via en anden platform, I allerede bruger.

CFCS anbefaler, at

- **Indkommende mails behandles i henhold til afsenderdomænets DMARC-politik.**
- **Antivirus installeres, mailfiltre bruges, og de løbende opdateres.**
- **Mails indeholder ikke links til websider, hvorfra der er direkte login med NemID eller andre loginløsninger.**
- **Mængden af tilgængelig information om organisationen og medarbejderne begrænses.**
- **Der udarbejdes processer, der kan bidrage til at reducere risikoen fra phishing-angreb, for eksempel, processer for pengeoverførsler.**
- **Afsenderen kontaktes på anden vis for at få bekræftet afsenderens identitet og ægtheden af mailen, hvis der er mistanke om phishing-forsøg.**
- **Der er processer til nem rapportering om mulige phishing-forsøg.**
- **Der anvendes DMARC, SPF og DKIM.**
- **Medarbejderne er introduceret til kommunikationspolitik, og at phishing-lignende kommunikation undgås i både intern og ekstern kommunikation.**

Begræns konsekvenserne af ikke opdagede phishing-angreb

Phishing-mails vil ofte indeholde skjult malware eller linke til en hjemmeside med malware. Hvis modtageren klikker på linket i mailen eller åbner den vedhæftede fil, kan der potentielt blive installeret og aktiveret skadelig kode på modtagerens enhed.

Valget af konkrete sikringsstiltag afgøres af behov og arbejdsmetoder i jeres organisation. I de følgende afsnit beskrives en række overordnede tiltag, I bør overveje.

Installer sikkerhedsopdateringer og anvend application control
Ved at holde jeres systemer og enheder opdateret med de seneste sikkerhedsopdateringer, forhindres hackerne i at udnytte kendte sårbarheder.

I kan også overveje at bruge application control løsninger. De sikrer, at kun autoriserede programmer kan aktiveres på enheden. Teknikken kan være med til at begrænse konsekvensen, hvis brugeren klikker på en vedhæftet fil eller på et link.

Hold antallet af brugere med lokale administratorrettigheder på et minimum
I bør begrænse antallet af brugere med lokale administratorrettigheder. Konti med lokale administratorrettigheder kan eksempelvis misbruges til at installere og aktivere uautoriseret software som malware. Derfor er en begrænsning af antallet af de kontotyper med til at forhindre, at brugere ved et uheld kommer til at installere malware fra en phishing-mail.

Administrative konti bør ikke bruges til at tjekke mails og til at gå på internettet med. Almindelige bruger konti bør benyttes i stedet. Derudover bør kritiske netværk ikke indeholde mailklienter.

Implementer tiltag, der beskytter brugere mod kendte ondsindede hjemmesider
Som tidligere nævnt kan der blive installeret og aktiveret skadelig kode på modtagerens enhed, hvis modtageren klikker på linket i en phishing -mail. Phishing-mails kan også indeholde links til falske loginsider. Her vil hackeren forsøge at få modtageren til at indtaste sit brugernavn og password for at skaffe sig adgang til, eksempelvis, interne it-systemer med kritiske forretningsmæssige informationer. Men hvis det ikke er muligt at tilgå hjemmesiden, så vil angrebet ikke kunne udvikle sig.

Et tiltag kan være brugen af en sikker DNS-tjeneste, da denne blokerer for domæner, der er kendt for eller vurderet til at være ondsindede.

DNS er en forkortelse for **Domain Name System**. DNS kan man nærmest kalde for internettets telefonbog. En bruger tilgår information online gennem domænenavne, fordi det er noget, der er simpelt for mennesker at huske. Internetbrowsere interagerer gennem IP-adresser. DNS oversætter domænenavnene til IP-adresser, sådan at browsere kan indlæse internetressourcer.

Det er et krav for statslige myndigheder, at de anvender en sikker DNS-tjeneste eller implementerer en anden løsning til beskyttelse mod skadelige hjemmesider.

Organisationen kan også bruge en proxy-service til at blokere for forsøg på at få adgang til domæner, der er kendte malware- og phishing-sider. Proxy-servicen kan også bruges til at blokere for domæner, der ikke overholder organisationens politikker.

Brug flerfaktor-autentifikation
Hvis en hacker har fået lokket brugernavn og password ud af en medarbejder, kan brugen af flerfaktor-autentifikation forhindre, at hackeren får adgang til den specifikke konto eller system.

Der findes flere forskellige flerfaktor-autentifikations metoder. Hvilken metode, der passer bedst til den enkelte organisation eller det enkelte formål, afhænger blandt andet af jeres sikkerhedskrav, og hvilke ressourcer I har tilgængelige til administration og teknologi.

Flerfaktor-autentifikation

Flerfaktor-autentifikation er en loginproces hvor brugeren får adgang ved at identificere sig (eksempelvis brugernavn) og to eller flere af:

- Noget brugeren ved (f.eks. pinkode eller password),
- Noget brugeren har (f.eks. ID-kort, mobiltelefon, nøglekort, eller USB-sikkerhedsnøgler),
- Noget brugeren er (f.eks. ansigtsgenkendelse eller fingeraftryk), kaldes også biometrisk identifikation.

Oftest benyttes flerfaktor-autentifikation, hvor eksempelvis et password (noget brugeren ved), suppleres med godkendelse på mobiltelefonen (noget brugeren har).

CFCS anbefaler, at

- **Systemer, programmer og enheder bliver opdateret med de seneste sikkerhedsopdateringer.**
- **Application control løsninger anvendes til at sikre at kun autoriserede programmer aktiveres på enheden.**
- **Der implementeres tiltag som sikker DNS til at beskytte brugerne mod kendte ondsindede hjemmesider.**
- **Der anvendes flerfaktor-autentifikation hvor muligt.**

Håndter phishing-angreb

Alle organisationer vil på et tidspunkt skulle håndtere en sikkerhedshændelse forårsaget af et phising-angreb uanset hvor mange sikkerhedstiltag der er implementeret. Det vigtigste er at opdage hændelsen hurtigt, så den kan stoppes og konsekvenserne kan begrænses.

Logning
Organisationen bør have en politik for logning, som skal sikre at gode og anvendelige logs er tilgængelige. Samt at de er læsbare og rækker tilstrækkeligt langt tilbage i tid. Logning er vigtigt, fordi det er gennem logs, at det bliver muligt at undersøge it-sikkerhedshændelser.

I de tilfælde hvor en ekstern leverandør står for logningen, bør organisationen sørge for at stille krav til leverandøren om hvilke logs, der skal genereres hos partnere, og hvordan de logs kan tilgås. Det skyldes, at nogle leverandører kun foretager logning, hvis der er indgået specifikke aftaler herom.

Når det handler om phishing kan logs fra mailsystemer, inklusiv ind- og udgående gateways og spam/virus-filtreringstjenester, bidrage til at opdage og analysere phishingforsøg, levering af malware, og nogle metoder til eksfiltrering. Center for Cybersikkerhed anbefaler at man bør logge afsender/modtager mailadresser, navn og IP-adresse på afsender-/modtagergateways, emne, dato og coordinated universal time (UTC). Størrelse på besked og navne på vedhæftede filer kan eventuelt også logges.

Hændelses- og beredskabsplaner
Når I har opdaget en hændelse, er det vigtigt, at I ved, hvad I skal gøre. Derfor bør organisationen have konkrete planer for hændelseshåndtering og beredskab, der tydeligt beskriver, hvad der skal gøres og af hvem. Det er vigtigt, at planerne er kendt i organisationen, og at de bliver testet og opdateret regelmæssigt. Nogle af de konkrete aktiviteter, der kan indgå i planerne, er at nulstille og reetablere de berørte systemer.

I de tilfælde hvor en eller flere ydelser varetages af en leverandør, bør organisationen have aftaler på plads med leverandørerne i forhold til hændelseshåndtering og beredskab. Derudover bør beredskabsplanen indeholde kontaktoplysninger til jeres leverandører.

CFCS anbefaler, at

- **Der er en politik for logning, som sikrer at gode og anvendelige logs er tilgængelige.**
- **Der er planer for hændelseshåndtering og beredskab, og at de testes regelmæssigt.**

Referencer

Center for Cybersikkerhed (2021): *Cyberforsvar der virker*

Center for Cybersikkerhed og Digitaliseringsstyrelsen (2022): *Cybersikkerhed i leverandørforhold*

Center for Cybersikkerhed (2020): *Cybertruslen fra phishing-mails*

Center for Cybersikkerhed (2022): *DMARC*

Center for Cybersikkerhed (2020): *Logning – en del af et godt cyberforsvar*

Center for Cybersikkerhed (2020): *Passwordsikkerhed*

National Cyber Security Centre (2019): *Phishing attacks: defending your organisation*