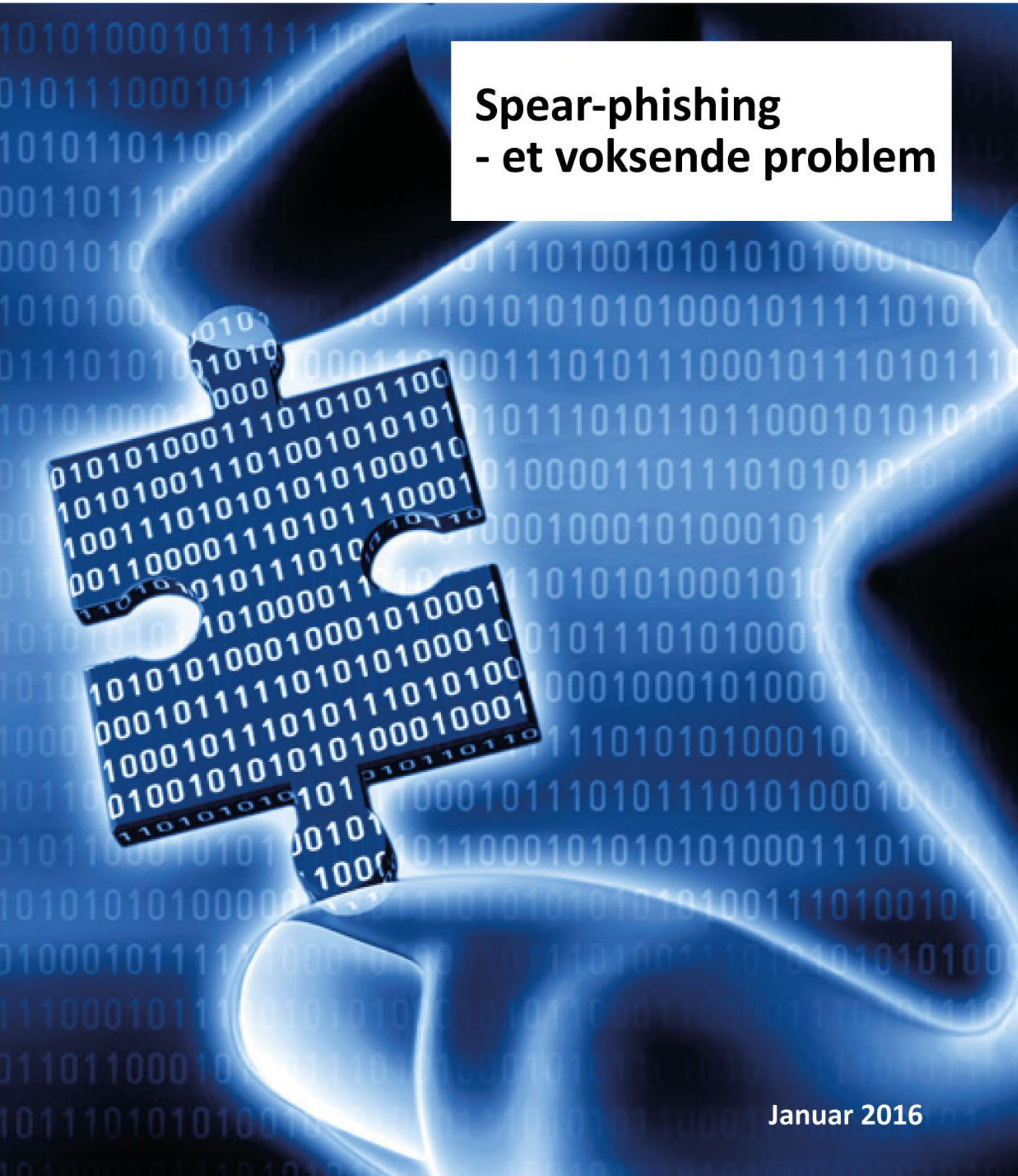
CENTER FOR CYBERSIKKERHED

Sikkerhedsvejledning

Spear-phishing - et voksende problem



Januar 2016

Baggrund

Center for Cybersikkerhed har erfaret, at flere danske virksomheder bliver ramt af phishing og spear-phishing-angreb.

Phishing vs. Spear-phishing

Populært beskrevet er et phishing-angreb et angreb, hvor der "skydes med spredehagl", mens et spear-phishing er et målrettet angreb rettet mod enkelt-individer.
Succesraten for, at et spear-phishing-angreb lykkes er langt højere end for et almindelig phishing–angreb.

Phishing

En phishing-kampagne er generelt karakteriseret ved, at der udsendes en meget stor mængde enslydende mails til en bred personkreds. Hensigten er at manipulere modtagerne til at åbne vedhæftede filer eller klikke på indlejrede links i en fremsendt mail.

- For angriberen er det et spørgsmål om at gøre de fremsendte mails tillokkende og umiddelbart overbevisende for modtageren. Dette sker typisk ved, at: anvende officielle navne og logoer på virksomheder og myndigheder, som er kendt i det offentlige rum. Det kan være banker, betalingskortselskaber, forsikringsselskaber, kurervirksomheder, postvæsenet m.fl.
- mailen indeholder informationer, der er meget tillokkende for modtageren, eller kræver akut handling.

Et andet karakteristika er, at de ondsindede mails ofte er formuleret på et meget dårlig dansk, og de danske bogstaver æøå kan være erstattet af ae, oø og aa.

Sådan kan en phishing-mail se ud:

POST

Du har uforløste pakken

Vi har modtaget din pakke **CT54916560DK** på **2015/09/15**. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Anvendelsen af Post Danmarks firmalogo er udelukkende et udtryk for, at logoet har været misbrugt i denne phishing-kampagne.

Formålet med et phishing-angreb er typisk at franarre modtageren fortrolige oplysning i form af adgangskoder, kontooplysninger eller engangsnøgler (f.eks. kopi af NemID nøglekort). Se også www.borger.dk/sikkerpånettet

Spear-phishing

Et spear-phishing-angreb er målrettet enkeltpersoner i en organisation. Formålet kan være at hente fortrolige forretningsoplysninger, bruger-id og adgangskoder til konti mv. ud af organisationen. Disse oplysninger vil så - sammen med en mulig infektion af modtagerens computer, tablet eller mobiltelefon - kunne anvendes i forbindelse med et decideret cyber-angreb mod organisationen.

Et typisk spear-phishing-angreb udsendes ofte kun til få udvalgte personer, og for angriberen vil det normalt kræve en vis rekognoscering at sikre, at den fremsendte mail virker relevant, overbevisende og tillidsvækkende.

En spear-phishing mail er typisk karakteriseret ved, at:

- den fremsendte mail 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 typisk 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, og kan være på engelsk.
- der ikke optræder trusler eller på anden vis opfordring til presserende handlinger.

Billede nederst viser hvordan en spear-phishing-mail kan se ud.

Det må antages, at angriberen har afdækket, at modtageren er involveret i en ansættelsesproces, og at han i den forbindelse samarbejder med en Anne Andersen, der objektivt set godt kan have sendt modtageren sin vurdering af ansøgningskandidaterne. Når modtageren i dette tilfælde klikker på den vedlagte Excel-fil inficeres hans computer.

En nøjere kontrol – f.eks. en telefonopringning til Anne Andersen - vil afsløre, at den pågældende mail er afsendt af en ukendt tredjepart.

Uafhængig af om der er tale om en phishing eller en spear-phishing mail er formålet at lokke ofret til at klikke på en vedhæftet fil eller trykke på et indlejret link, hvorved modtagerens enhed potentielt bliver inficeret med malware.

Center for Cybersikkerhed har konstateret, at spear-phishing-angreb ofte lykkes på trods af, at organisationer i en vis udstrækning allerede har garderet sig imod spam mails og virusangreb.

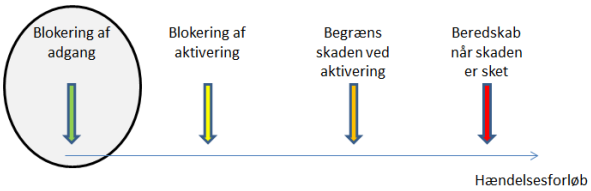
Det er svært – og til tider umuligt - at gardere sig 100 % imod et velgennemført spear-phishing-angreb. Men en efterlevelse af Top 4-sikringsforanstaltningene fra vejledningen "Cyberforsvar der virker" vil i betragtelig grad reducere risikoen for, at hackere får held med angrebet. Men disse sikrings-foranstaltninger bør ikke stå alene.

Organisationen bør satse på en række foranstaltninger, der for eksempel struktureres ud fra de faser, et spear-phishing-angreb normalt gennemgår. Således kan sikkerhedsforanstaltninger etableres ved, at:

1. blokere brugernes adgang til skadelige links, vedhæftede filer mv. ved at forhindre, at mailen kommer frem til brugeren.
2. blokere brugernes mulighed for at aktivere det skadelige indhold.
3. begrænse skaden, hvis brugeren faktisk aktiverer skadelig links, vedhæftede filer mv.
4. iværksætte et beredskab, hvis skaden er sket.

Disse tiltag vil blive beskrevet i det følgende.

Blokering af adgangen til skadeligt indhold



Generelt har organisationer anvendt spam- og virusfiltre i en række år, og det er i dag værktøjer, der er accepteret af medarbejderne. Disse filtre er i udstrakt grad baseret på mønstergenkendelse. Mails skannes, og hvis der i indholdet eller de vedhæftede filer findes et match i forhold til et allerede identificeret virusmønster, en specifik sprogbrug, typen af de vedhæftede filer mv., vil den pågældende mail blive sat i karantæne. I relation til filtyper har specielt .exe filer i lang tid været uønskede som vedhæftning, men det har også været muligt at indlejre eksekverbar kode i gængse programmer, som blandt andre Excel, Word, Adobe Reader.

Man bør endvidere overveje en blokering for modtagelse af .zip, .rar og .scr filer, fordi disse traditionelt set ofte anvendes ifm. specifikke angreb. Endvidere er det ofte kun en begrænset kreds af brugere, der har behov for at modtage disse vedhæftninger.

Top 4-sikringsforanstaltningene fra vejledningen "Cyberforsvar der virker":

- Opdater programmer, f.eks. Adobe Reader, Microsoft Office, Flash Player og Java, med seneste sikkerhedsopdateringer (klassificeret som højrisiko) inden for to dage.
- Opdater operativsystemet med seneste sikkerhedsopdateringer (klassificeret som højrisiko) inden for to dage. Undgå Windows XP eller tidligere.
- Begræns antallet af brugerkonti med domæne- eller lokaladministratorprivilegier. Disse brugere bør anvende separate uprivilegerede konti til e-mail og websurfing.
- Udarbejd positivliste over godkendte programmer for at forhindre kørsel af ondsindet eller uønsket software.

Problemet er imidlertid, at angriberne også har kendskab til disse filtre, og de tilpasser deres angreb, så de ikke fanges af filtrene. I relation til filtyper kan dette f.eks. ske ved, at man omdøber eller komprimerer (”zipper”) den vedhæftede fil en eller flere gange eller ændrer navnet på filtypen, så et simpelt filtypecheck omgås. Desværre vil disse forsøg på omgåelse i visse tilfælde føre til, at de fremsendte mails kommer igennem til brugeren. Anvender man i stedet en kontrol i filtret, der i større grad analyserer indholdet i de vedhæftede filer, så vil risikoen for, at de pågældende mails slipper igennem, være mindre.

Da antallet af potentielt skadelige filtyper er konstant voksende, kan man som alternativ til denne metode (black-listing) overveje, om man i stedet bør anvende en liste over godkendte filtyper (white-listing). White-listing understøttes af langt de fleste produkter og vil med stor sandsynlighed være nemmere at administrere end en blacklist.

Mange spamfiltre anvender i dag også blacklisting af domæner, således at mails afsendt fra specifikke domæner blokeres. Der eksisterer en række tjenester på nettet, hvor organisationer kan abonnere på blacklister over domæner, der erfaringsmæssigt er skadelige. Metoden er effektiv, men kan også have den uheldige konsekvens, at hæderlige organisationer kan få deres domæne blacklistet ved en fejl. Herved kan organisationer blive afskåret fra at kommunikere via mails til deres samarbejdsparter.

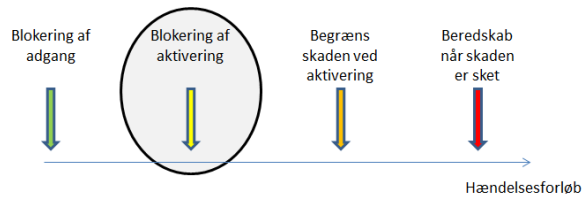
Med hensyn til begrænsningen af adgang til links i mails, der fører til, at modtagerens enhed inficeres, så skal denne begrænsning sikre imod malware indlejret i web-sider, bannere, reklamer, billeder mv.

For at imødegå risikoen for, at en bruger kan tilgå skadeligt indhold via et link i en modtaget mail, er der følgende muligheder for sikkerhedsforanstaltninger:

- Styring via etablerede politikker og retningslinjer for brug af mail og internettet, hvor organisationens forventninger til brugerenes adfærd beskrives. Foranstaltningen kan ikke stå alene.
- Fjernelse af alle hyperlinks i indkommende mails. Dette kan f.eks. ske i et antivirus filter. Et sådan tiltag vil af mange blive opfattet som særdeles restriktivt, hvorfor løsningen ikke er særligt udbredt. Blokering af legitim kommunikation vil også juridisk kunne udgøre et alvorligt problem.

Organisationen bør altid følge etableringen af sikkerhedsforanstaltninger op med uddannelse og oplysningskampagner rettet mod organisationens medarbejdere. Herved kan man skabe den nødvendige forståelse af, hvorfor organisationen har etableret de sikkerhedsforanstaltninger, der begrænser brugernes muligheder.

Blokering af aktivering



Hvis første sikringsniveau fejler og brugeren på trods af etablerede filtre og white- eller blacklister får adgang til links til eller filer med skadeligt indhold, hvilke muligheder har organisationen så for at blokere brugerens aktivering af det skadelige indhold?

Mulighederne er på dette niveau relativt begrænsede, og derfor handler det i høj grad om at påvirke brugerens adfærd i relation til, hvorledes modtagne mails skal håndteres.

Organisationen skal i stedet uddanne brugerne i god adfærd i forbindelse med mailhåndtering. Center for Cybersikkerhed anbefaler, at ledelsen sikrer, at alle medarbejdere uddannes i hvordan de opdager de uønskede mails. Dette bør ske gennem generel oplysning og gennemførelse af praktiske øvelser hvor medarbejderen konfronteres med forskellige eksempler på ondsindede mails. Sidst i denne vejledning er der vist et eksempel på, hvordan man afslører sådanne mails, men mange andre offentlige og private organisationer, herunder Digitaliseringsstyrelsen, SKAT og Nets har lignende vejledninger på nettet.

Ledelsen bør endvidere sikre, at der følges op, hvis en medarbejder gentagne gange har fejlhåndteret uønsket mails eller ignoreret advarsler (se nedenstående eksempel), der kan blive vist når brugeren klikker på en vedhæftet fil eller besøger en hjemmeside på nettet.

Det er samtidig vigtigt at opretholde en sund sikkerhedsadfærd, der sikrer, at brugerne indrapporterer modtagne phishing-mails, så it-organisationen kan advare resten af organisationen og den organisation eller myndighed, som bruges som uvidende afsender.

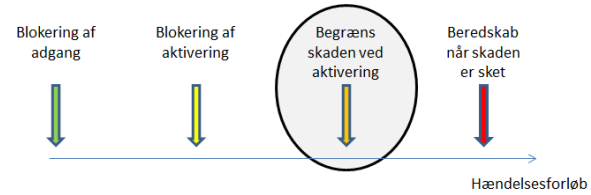
Ligeledes bør it-afdelingen/den juridiske afdeling være behjælpelige med at verificere eventuelle domæner, f.eks. hos DK Hostmaster. For domæner under .dk bør man være ekstra mistænksom, hvis et whois-opslag viser, at der er tale om en udenlandsk ejer, da valideringen af udenlandske domæneejere er begrænset og usikker.

Der kan også etableres tekniske foranstaltninger, der kan øge sikkerheden i netop denne fase af hændelsesforløbet. Anvendelse af domæne-blokeringer i en intern DNS-server (DNS Sink-hole) vil betyde, at alle forsøg på at tilgå indhold på erkendte problematiske domæner fejler, hvis brugeren trykker på et link til disse i en mail.

Et Sink-hole er en standard DNS-server, der er konfigureret til at uddele ikke routebare IP-adresser for domæner, der er registreret på DNS-serveren som uønskede. Herved vil en intern computer afskæres fra at besøge hjemmesider under disse domæner.
Jo højere op i DNS-hierarkiet, der blokeres, jo flere hjemmesider vil der blokeres adgang til.
Anvendelsen af et DNS-Sink-hole skal ske sammen med en styring af de interne computeres adgang til DNS-opslag. I modsat fald vil et DNS-Sink-hole ikke have nogen effekt.

Blokeringen af adgangen kan også implementeres i såvel firewall som proxyservere, som brugernes trafik passerer igennem. Afhængig af den konkrete installation kan en sådan løsning være mere eller mindre omkostningskrævende i forhold til hvor mange ressourcer, der er nødvendige for at holde løsningen ajour og dermed sikker.

Begræns skaden ved aktivering



Hvis medarbejderen på trods af de tidligere beskrevne foranstaltninger alligevel bevidst eller ubevidst aktiverer et link til eller en fil med skadeligt indhold, er det vigtigt, at der er etableret sikringsforanstaltninger, der forhindrer eller begrænser konsekvensen af denne handling.

Samtidig er det vigtigt, at organisationen etablerer en kultur, hvor det er acceptabelt at begå fejl, således at den enkelte medarbejder ikke er tilbageholdende med at anmelde, at man har klikket på et "farligt" link, eller at man har åbnet en vedhæftet fil med problematisk indhold. Hermed kan organisationen hurtigt iværksætte foranstaltninger med henblik på at begrænse en mulig skade.

Følgende tekniske sikringsforanstaltninger vil i denne situation samtidig være relevante at implementere:

- Opdatering af operativsystem og applikationer.
- Applikations-white-listing, der sikrer, at ikke autoriserede programmer aktiveres på pc'en.
- Begrænsning af brugeres privilegier lokalt på pc'en samt til organisationens øvrige systemer og informationer.
- Aktivering af "click-to-run" for Adobe Flash, Silverlight og Java, så disse objekter ikke afvikles automatisk på enheden, der besøger en hjemmeside.
- Opdatering af aktiv virusbeskyttelse.

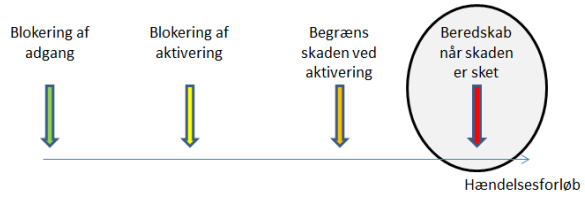
Nogle af disse foranstaltninger er beskrevet i Center for Cybersikkerheds vejledning om "Cyberforsvar der virker". Disse sikringsforanstaltninger anses for at være fundamentalt vigtige for beskyttelse af organisationen imod cybertrusler, herunder spear-phishing-angreb.

I forhold til en decideret applikations-white-listing vil en begrænsning i funktionaliteten af brugerens anvendte browser være et mindre restriktivt skridt på vejen. Sådanne foranstaltninger kan medføre, at specifikke indholdstyper ikke kan vises (f.eks. Adobe Flash objekter, der som regel kan blokeres uden store konsekvenser eller Oracle Java kode).

Uafhængig af om det er begrænsninger i browseren eller en fuld applikations-white-listing vil det være organisationens ledelse, der skal tage stilling til, om organisationen som helhed kan leve med disse begrænsninger, eller om man ønsker en differentieret, centraliseret styring med dertil øgede administrative omkostninger.

Ligegyldig om en begrænsning sættes ind i firewall, mail/web-filtre eller på pc-platformen skal man være opmærksom på, at der hos nogle brugere er stor kreativitet i at omgå begrænsningerne. I nogle tilfælde kommer man endvidere ud for, at legale sider eller legalt indhold blokeres - måske på grund af et lidt for "firkantet" regelsæt. En sådan blokering vil juridisk kunne udgøre et problem.

Beredskab hvis skaden er sket



Hvis organisationen er blevet ramt af et spear-phishing-angreb, kan denne strukturerede guide følges:

1. *Inddrag de rette personer.*
   - Inddrag straks topledelsen og de relevante tekniske kompetencer, herunder specialister udefra, hvis organisationen ikke selv råder over den fornødne viden.

2. *Stands ulykken*
   - Etabler et hurtigt overblik over, hvilke systemer og data, der er ramt, og hvornår det er sket. Dette kan være yderst vanskeligt, da visse typer angreb netop tilstræber at være så "usynlige" som muligt.
   - Sluk eller isoler alle ramte systemer så hurtigt som muligt. Hvis organisationen er i tvivl, er det bedre at stoppe et system for meget end et for lidt.

3. *Iværksæt om nødvendigt nøddrift*
   - Gå ud fra, at nulstilling og reetablering af systemerne kommer til at tage lang tid.
   - Informer organisationen om situationen og etabler om nødvendigt nøddrift for kritiske systemer.

4. *Oprensning og reetablering*
   - De berørte systemer startes op enkeltvis på et isoleret netværk.
   - Foretag om nødvendigt en komplet reinstallation af de specifikke systemer (operativsystemer og applikationer).
   - Indlæs konfigurationer og data fra sikkerhedskopier, der er blevet taget, før systemet blev inficeret.
   - Kontroller de reetablerede systemer og data og tag en ny sikkerhedskopi.
   - Overfør det reetablerede system til produktion.

5. *Opfølgning og læring*
   - Udarbejd eller opdater organisationens politik og retningslinjer for, hvordan medarbejdere skal forholde sig til mails med vedhæftede filer og sørg for, at det ofte kommunikeres ud i organisationen.
   - Etabler om nødvendigt yderligere tekniske foranstaltninger til blokering af malware.
   - Vurder på baggrund af den aktuelle hændelse, om den etablerede back-up-plan lever op til forventningerne. Indarbejd og implementer om nødvendigt eventuelle reviderede krav.
   - Gennemfør periodiske øvelser, hvor medarbejdere trænes i at identificere og undgå spear-phishing-angreb.

Hvorledes spotter man en (spear-)phishing-mail:

6. **Ukendt eller falsk afsender.** Det er muligt at udarbejde en mail, hvor den synlige afsender er forskellig fra den virkelige afsender (simpel form for spoofing). Kontroller derfor de skjulte oplysninger. I Outlook kan dette gøres ved at flytte markøren over afsenderen, herved adressen på afsenderen vises. Denne funktion er desværre ikke mulig i alle mail-klienter.

7. **Kontroler mailens egenskaber.** Ved en kontrol af egenskaberne i mail headeren for en mail, vil det kunne afsløres, hvorfra en mail er afsendt (Se eksemplet på næste side). I Outlook kan disse oplysninger findes under fanen "Filer". Bemærk, at man ved et veludført spear-phishing-angreb, hvor afsenderen selv er kompromitteret, ikke afslører noget mistænksomt ved denne metode.

8. **Falske hyperlinks.** Hyperlinks i mailen peger på andre domæner end dem, der er vist. Domænet kan kontrolleres ved f.eks. i Outlook at føre markøren over på de enkelte links. Herved vises det bagvedliggende domæne.

9. **Underlige navne på vedhæftede filer.** Det ses ofte, at phishing-mails har vedhæftede filer, der er navngivet på en måde, der slører den egentlige filtype. Eksempelvis kan dette ske ved anvendelsen af mange blanktegn som i filnavnet: "Personaleændringer.pdf .exe"

1. **Dårligt sprog og stavning.** Phishing-mails er ofte oversat automatisk eller af personer uden kendskab til dansk.

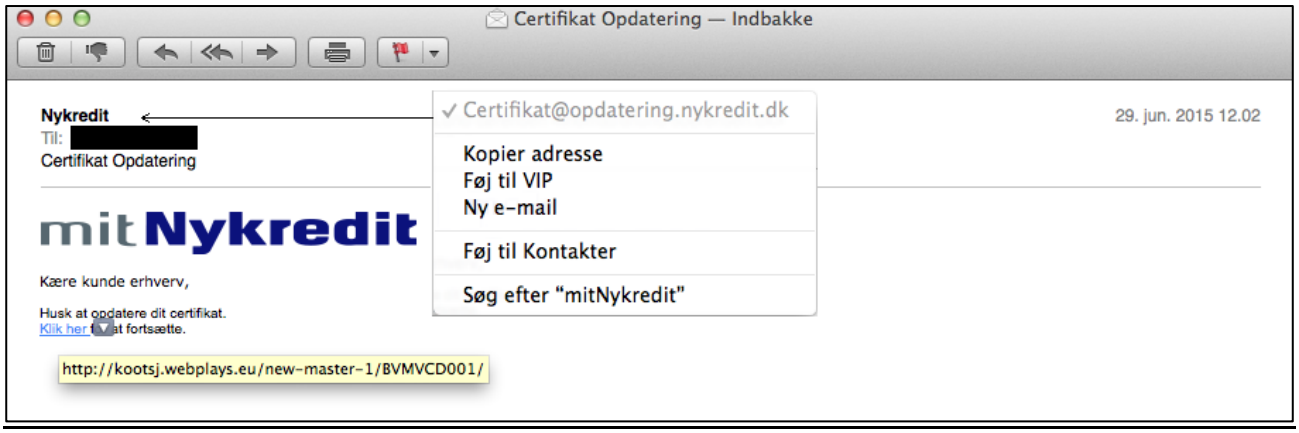
2. **Opfordring til umiddelbar handling.** I mange phishing-mails opfordres brugeren til at kontakte en hjemmeside eller at indsende oplysninger øjeblikkeligt. Er du i tvivl, så kontakt afsender direkte f.eks. via telefon og spørg ind til henvendelsen.

3. **Udlevering af personlige oplysninger.** Ingen troværdig part vil opfordre til, at man fremsender personlige oplysninger i en almindelig mail. Her bør man ligeledes kontakte afsender direkte, f.eks. via telefon, og spørge ind til henvendelsen.

4. **Vindere af lotteri eller overdragelse af formue.** Denne form for phishing-mails (også kaldt Nigeria-breve) er havnet hos mange brugere, der i god tro har udleveret oplysninger og indbetalt penge til svindlere. Mails om ukendte lotterier eller lignende bør slettes straks.

5. **Skadelige vedhæftede filer.** Åben aldrig en vedhæftet fil, medmindre du er fuldstændig klar over, hvad den vil indeholde. Kontakt om muligt den umiddelbare afsender via telefon med henblik på en verifikation af indholdet.

Følgende er et eksempel på en phishing-mail, hvor den umiddelbare afsender ser korrekt ud, men hvor egenskaberne på det angivne link (vist i mailen som "Klik her") afslører, at der er tale om en falsk mail.



Anvendelsen af Nykredits firmalogo er udelukkende et udtryk for at logoet har været misbrugt i denne phishing-kampagne.

At der er tale om en falsk afsenderadresse "Certifikat@opdatering.nykredit.dk" afsløres ligeledes hvis man ser nærmere på egenskaberne i mail headeren for den specifikke mail, der i virkeligheden er afsendt fra domænet "shankeshjewellers.com".