COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

TLP:WHITE

Pak phishing aan

-

Maatregelen voor effectieve preventie

Inhoud

1 Phishing

Phishing is een van de meest voorkomende vormen van internetfraude. Bij phishing probeert een aanvaller de inloggegevens of andere gevoelige gegevens van een slachtoffer buit te maken. Dit doet de aanvaller door een bericht, meestal een e-mail, te sturen die een link naar een malafide website bevat. Deze website toont dan een inlogpagina. Wanneer het slachtoffer zijn of haar gegevens hier invult, worden deze naar de aanvaller verstuurd, die deze vervolgens kan misbruiken voor allerlei doeleinden.

Andere vormen van phishing pogen om een slachtoffer malware uit te laten voeren, geld over te laten maken, een creditcardnummer of andere persoonlijke gegevens te achterhalen, et cetera.

Dit whitepaper gaat over het bestrijden van phishing naar inloggegevens via e-mail, al zijn sommige van deze technieken ook geschikt voor het beschermen tegen andere vormen van phishing. Z-CERT wil haar deelnemers en het Nationaal Cyber Security Centrum bedanken voor de bijdragen aan de totstandkoming van dit whitepaper.

1.1 Doel en doelgroep

Met dit whitepaper wil Z-CERT zorginstellingen helpen phishing pogingen via e-mail aan te pakken. Dit stuk is geschreven voor (Chief) Information Security Officers, Information Security Managers, en het daarbij behorend uitvoerend personeel, om een start te kunnen maken met het bestrijden van phishing.

1.2 Wat ziet Z-CERT?

Op het moment van schrijven valt een aanzienlijk deel van de incidenten die gemeld worden bij Z-CERT in de categorie ‘phishing’. Z-CERT is daar niet de enige in, Microsoft rapporteerde onlangs dat het aantal phishing berichten met 250% steeg tussen januari en december van 2018[1]. Veel van de phishing campagnes die Z-CERT ziet, maken gebruik van dezelfde methodieken. Met dit document wil Z-CERT u helpen om phishing in uw organisatie aan te pakken.

Methodieken

Gebruikers lukt het vaak niet om URL’s in phishing e-mails te herkennen als malafide. Aanvallers gebruiken verschillende manieren om de echte URL ‘onzichtbaar’ te maken.

- URL’s worden gemaskeerd door het gebruik van URL-shorteners. Hierdoor is in een e-mail de daadwerkelijke URL niet te achterhalen.
- De URL die zichtbaar is in de mail leidt via een redirect naar een andere URL.
- De URL verwijst naar een domeinnaam die één letter afwijkt van de echte domeinnaam, zoals bijvoorbeeld: zieke**m**huis.nl
- De URL bestaat uit meerdere ‘lagen’ zoals bijvoorbeeld: login.ziekenhuis.nl.inlog.sk.

De websites waar phishing e-mails naar toe leiden, vallen uiteen in een aantal categorieën. Het verschilt van categorie tot categorie welke maatregelen effectief zijn. Z-CERT ziet de volgende vormen:

1 Microsoft Security Intelligence Report Volume 24

- websites gemaakt voor phishing en gehost op het domein van gratis hostingpartijen;
- websites gemaakt voor phishing en gehost bij legitieme, betaalde hostingpartijen; en
- legitieme websites die gecompromitteerd zijn.

Voor het overgrote deel gebruiken aanvallers gratis hostingpartijen. Z-CERT ziet maar zelden phishing die gebruikmaakt van legitieme websites die gecompromitteerd zijn.

1.3 Impact

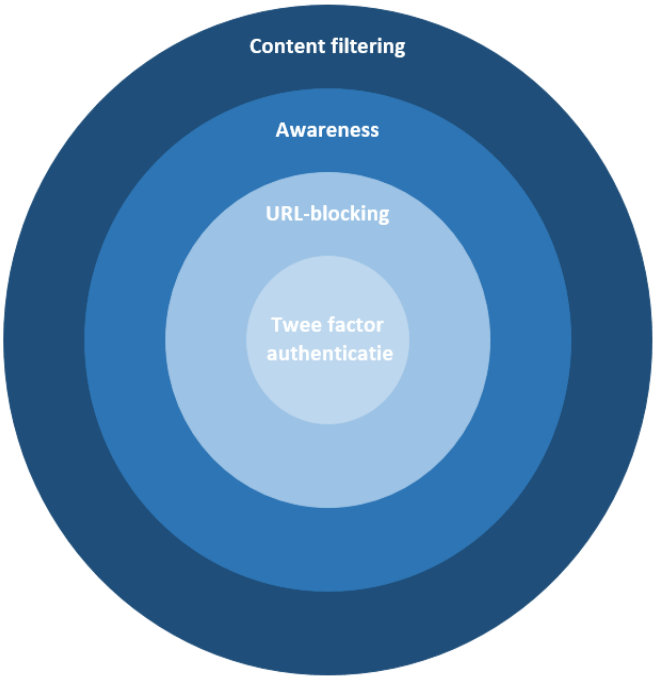
Een succesvolle phishing campagne kan voor grote schade zorgen. De verkregen inloggegevens kunnen bijvoorbeeld gebruikt worden om malafide e-mail te versturen vanuit een webmail omgeving. Een aanvaller zou ook gebruik kunnen maken van niet gepatchte kwetsbaarheid, of een slechte configuratie, om vanuit de webmail-omgeving verder in het netwerk door te dringen.

Maar niet alleen het misbruiken van de toegang kan voor schade verzorgen. Het inloggen op zichzelf zorgt al voor problemen. Misschien heeft de aanvaller wel gevoelige (persoons)gegevens ingezien en is een melding bij de Autoriteit Persoonsgegevens nodig. Hierdoor is alleen het resetten van een wachtwoord niet voldoende, zeker niet als niet kan worden uitgesloten dat de aanvaller gegevens heeft ingezien.

2 Maatregelen

De meeste phishing campagnes maken gebruik van dezelfde technieken. U kunt dus maatregelen selecteren die daar goed tegen werken. De maatregelen uit dit document kunnen u goed op weg helpen. Deze maatregelen zijn weergeven in een schillen-model. Op verschillende punten kunt u maatregelen treffen. Hierdoor neemt de kans op een succesvolle phishing aanval sterk af.

Het is van belang dat u zorgvuldig afweegt welke oplossing passend is voor uw organisatie. Tevens zijn de beschreven maatregelen niet de enige te nemen maatregelen. Of de enige maatregelen die invloed hebben op het succes van phishing aanvallen. Maatregelen die uit risicoanalyses blijken kunnen ook van invloed zijn.



Figuur Schilleni-model maatregelen

2.1 Content filtering

2.1.1 Wat is het

Content filtering is een maatregel om e-mail te screenen op bepaalde kenmerken of termen. E-mail- en antivirusprogramma's bieden deze functionaliteit. Afhankelijk hiervan wordt een score toegewezen aan de e-mail. Het e-mailsysteem of het antivirusprogramma dat de content filtering uitvoert, verplaatst, verwijdert of accepteert e-mail op basis van deze score. Hiermee houdt u een deel van de phishing e-mails en spam tegen. Content filtering an sich heeft slechts beperkte waarde. Er zijn zoveel typen aanvallen dat content filtering het best ingezet kan worden voor specifieke campagnes. Daarnaast kan content filtering voor enige ruis zorgen. Vertrouw daarom niet enkel op content filtering.

2.1.2 Inventariseren

Leg een lijst aan van terugkerende termen en teksten in ongewenste e-mails. Bijvoorbeeld: phishing campagnes die vanuit het Engels zijn vertaald, maken in de onderwerpregel soms gebruik van de term 'merk op' (Engels: 'notice'). In Nederlandse e-mail zou 'merk op' minder snel worden gebruikt in de onderwerpregel. Hierdoor zou dit aangemerkt kunnen worden als een verdachte term. Z-CERT levert bij actieve phishing campagnes zogenaamde Indicators of Compromise(IoC's) aan die u hiervoor kunt inzetten. Een IoC is een kenmerk, zoals een woord, onderwerpregel, domeinnaam of IP-adres, die ofdat u kunt gebruiken om detectie en filtering toe te passen.

2.1.3 Implementatie

Test content filtering zorgvuldig met de door u gekozen applicatie. Een te streng ingestelde content filtering kan ervoor zorgen dat legitieme e-mail niet meer aankomt. Een waarschuwing instellen in plaats van compleet filteren kan ook verstandig zijn. Gebruik hiervoor de lijst die u heeft aangelegd.

2.2 Awareness

2.2.1 Belang

Als phishing e-mails door de content filtering heenkomen, is het aan de gebruiker om deze te herkennen. Phishing e-mails hebben immers alleen effect als de gebruiker ze niet herkent of 'blindelings' op de link klikt. In informatiebeveiliging haalt men dan ook vaak aan dat 'de mens de zwakste schakel is'. Hoewel dit vaak onterecht is, hebben gebruikers een belangrijke rol in het herkennen van phishing en andere malafide e-mail wanneer de technologie tekortschiet. Hierom is het van belang dat uw medewerkers zich bewust zijn van de mogelijke risico's, dat zij de juiste middelen hebben om phishing e-mails te herkennen en daar adequaat mee om kunnen gaan. Zo kunt u medewerkers inzetten om uw organisatie veiliger te maken.

2.2.2 Inventariseren

Een mogelijke start van een awareness programma is om doormiddel van een eigen gesimuleerde phishing campagne een beeld te krijgen van het niveau van uw medewerkers, ofwel een nulmeting. Hiermee heeft u een uitgangspunt. Wat is de klik ratio in uw organisatie? Is dit hoger of lager in bepaalde afdelingen? Wordt er alleen geklikt? Of vullen medewerkers ook hun gegevens in? Melden medewerkers het als ze phishing e-mails krijgen?

2.2.3 Implementatie

Start een interne phishing campagne met diverse aanvalsmethoden. Denk hierbij aan e-mails met een phishing URL, een bijlage met macro's[2] of een verzoek om geld over te maken. Kies hierbij de ontvangers zorgvuldig. Voor de awareness is het goed om leidinggevenden, medewerkers en afdelingen bijvoorbeeld apart te behandelen. Probeer hierbij een aantal statistieken, gescheiden in afdelingen, in beeld te krijgen.

- Hoeveel medewerkers klikken op de link?
- Hoeveel medewerkers vullen hun gegevens in op de website?
- Hoeveel medewerkers openen de bijlage?
- Hoeveel medewerkers controleren of betaalverzoeken legitiem zijn?
- Hoeveel medewerkers melden de phishing poging?

Op basis van deze cijfers kunt u gericht actie ondernemen. Bedenk dat een constructief bericht aan het eind van de eigen campagne ook voor awareness kan zorgen. Een bij Z-CERT aangesloten deelnemer meldde een tijdelijke verhoging van de instroom van meldingen na een phishing campagne van meer dan 50%. Dat deze verhoging tijdelijk was, toont echter wel aan dat deze maatregel niet eenmalig getroffen kan worden.

Z-CERT adviseert om interne gesimuleerde phishing campagnes te voorzien van een informerend karakter. Het kan logisch lijken om alle medewerkers die erin zijn getrapt, streng toe te spreken en op training te sturen. Een betere oplossing is om melders te belonen door middel van een vermelding, kaart of cadeaubon. Hiermee koppelt u iets positiefs aan het detecteren en melden van phishes. Zorg dat niet bekend wordt welke medewerkers in de phishing e-mail getrapt zijn. Van hun vergissing kan uw organisatie immers leren.

[2] Als macro's in uw organisatie zijn toegestaan.

Train medewerkers middels bewustzijnscampagnes hoe men phishing e-mails kan herkennen. U kan hiervoor gebruik maken van posters of interne phishing campagnes.

Zorg er tevens voor dat medewerkers phishes, en andere verdachte e-mails, gemakkelijk kunnen melden door de toevoeging van een knop in het e-mailprogramma of het instellen van een speciaal e-mailadres. Laat deze meldingen naar een centraal punt gaan waar uw security medewerkers / IT helpdesk deze kunnen correleren en afhandelen. Hiermee worden campagnes inzichtelijk en hoeft er per incident maar één keer een analyse gedaan te worden. Bedank iedereen die berichten doorstuurt, ook als ze deze onterecht als phishing of malafide hebben aangemerkt. Dit verhoogt de meldingsbereidheid.

Blijkt dat een verdachte e-mail bij nader inzien toch legitiem is? Contacteer dan de verzender van de e-mail, zeker als dat een leverancier of interne partij is. Immers, als verzenders in legitieme e-mails vragen om inloggegevens, wordt het moeilijker voor een ontvanger om phishing e-mails te herkennen. U kunt hiervoor gebruikmaken van de NCSC-factsheet 'Goede bulkmail lijkt niet op phishingmail'[3].

Als een doorgestuurd bericht daadwerkelijk een phishing e-mail blijkt te zijn, vragen wij u de kenmerken daarvan te delen met Z-CERT. Z-CERT kan deze kenmerken delen met andere zorginstellingen. Hiermee kunnen actieve phishing campagnes sneller gestopt worden.

2.3 URL-blocking

2.3.1 Wat is het

Met phishing e-mails probeert een aanvaller gebruikers naar een malafide website te leiden om zo hun gegevens afhandig te maken. Als een gebruiker niet naar de malafide website kan, stopt de aanval. Het is daarom verstandig om het bezoek van bepaalde websites te blokkeren. Dit is in het bijzonder effectief omdat veel phishing campagnes gebruik maken van dezelfde websites. Zo zou een campagne de ene keer gebruik kunnen maken van 'asd86gad.websitemaker.com' en een andere keer van 'iohlkj123nb.websitemaker.com'. Door '*.websitemaker.com' te blokkeren, kunnen in een keer alle phishing campagnes die gebruik maken van dat domein gestopt worden. Tevens kan er overwogen worden om niet alleen domeinen te blokkeren maar ook zogenaamde 'topleveldomeinen' of TLD's. TLD's zijn de 'extensie' van een website, zoals ".com", ".ru" en ".nl". Immers, hoe vaak krijgt uw instelling berichten vanuit, of bezoeken uw medewerkers websites uit, Nigeria met het TLD ".ng"?

2.3.2 Inventariseren

Onderzoek of in uw organisatie legitiem gebruik wordt gemaakt van generieke websitehosters, URL-shorteners en buitenlandse sites.

2.3.3 Implementatie

Besluit hoe u wilt omgaan met het blokkeren van URL's. Wilt u deze allemaal blokkeren en ze alleen op aanvraag toestaan? Of wilt u gebruikers enkel waarschuwen als ze dergelijke sites bezoeken? Het is verstandig om een procedure te hebben om gemakkelijk URL's te kunnen blokkeren als u deze krijgt aangeleverd door Z-CERT. Bedenk hierbij dat het mogelijk is dat

[3] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-goede-bulkmail-lijkt-niet-op-phishingmail

in het beleid van uw organisatie staat dat websites niet, of niet zomaar, mogen worden geblokkeerd. Stem daarom met de verantwoordelijken een proces af om malafide websites snel te kunnen blokkeren.

Als u besluit om TLD's te blokkeren kan het goed zijn om in eerste instantie alleen waarschuwingen in te stellen zodat u een beeld kan krijgen van het gebruik van buitenlandse websites en de communicatie met het buitenland.

2.4 Multifactor authenticatie

2.4.1 De risico's

Het gebruik van multifactor authenticatie verlaagt de impact van een succesvolle phishing aanval aanzienlijk. Veel organisaties bieden, naast op afstand kunnen werken, webmail aan. Hiermee kunnen medewerkers op afstand hun mail lezen en versturen. Hier staat echter niet altijd multifactor authenticatie op ingesteld. Hierdoor kunnen aanvallers, als een phishing aanval geslaagd is, op afstand inloggen op de webmail om bijvoorbeeld spam te versturen, proberen verder het netwerk binnen te dringen of om e-mail te lezen.

2.4.2 Inventariseren

Onderzoek wat voor uw organisatie een werkbare oplossing is. Zo zou u gebruik kunnen maken van fysieke authenticatiesleutels, authenticatie apps op telefoons met codes of goedkeuringsvensters of van e-mails met een verificatiecode. De NCSC-factsheet Gebruik tweefactorauthenticatie[4] bevat hiervoor een aantal praktische handvatten. Onderzoek ook welke van de in de organisatie gebruikte applicaties en systemen tweefactor authenticatie en Single-Sign-On (SSO) ondersteunen.

2.4.3 Implementatie

Zorg voor een werkbare implementatie. Bij iedere inlogpoging een tweede factor vragen zou het zorgproces in de weg kunnen staan en irritatie oproepen bij medewerkers. Alleen aan het begin van de dag een tweede factor vragen is niet voldoende[5]. Draai een pilot met enkele medewerkers om te bepalen wat een werkbare sessie-tijd is en of de oplossing werkbaar is.

Bedenk dat multifactor authenticatie niet alleen bij webmail kan worden ingezet, maar ook op andere plekken in de organisatie. Z-CERT raadt aan om, waar mogelijk, gebruik te maken van SSO om medewerkers toegang te geven tot applicaties.

[4] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie
[5] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patiëntendossiers

3 Handelingsperspectief

Uiteraard is het mogelijk dat, ondanks het treffen van maatregelen, een phishing poging succesvol is en een aanvaller inloggegevens buitmaakt. Het kan moeilijk zijn om dit te detecteren. FireEye rapporteerde in haar M-Trends 2019 rapport[6] dat in Europa, van eerste entree tot exit / verwijdering, een hacker gemiddeld 177 dagen aanwezig is in een gecompromitteerd systeem.

Indicaties dat inloggegevens mogelijk in handen zijn geraakt van kwaadwillenden:

- inlogpogingen buiten kantooruren;
- inlogpogingen van buitenlandse IP-adressen;
- grote hoeveelheden verzonden e-mail;
- veranderde wachtwoorden;
- ongebruikelijk netwerkverkeer van medewerkers; en
- alle binnenkomende e-mail op een account wordt doorgestuurd / naar de prullenbak gestuurd.

Om bovenstaande indicatoren op te merken is het van belang om met enige regelmaat loggegevens te onderzoeken. Werk daarnaast goed samen met uw IT-helpdesk. Zij moeten extra bewust zijn t.a.v. phishing. Melden medewerkers bijvoorbeeld ‘vreemde’ incidenten bij de information security manager?

Hoewel dit whitepaper zich voornamelijk richt op misbruik van inloggegevens op de e-mail, is het mogelijk dat kwaadwillenden uit de e-mailomgeving proberen te ‘breken’. Neem deze mogelijkheid mee in uw risicoanalyses en tref bijpassende maatregelen zoals virtualisatie, applicatie whitelisting en blokkeren van macro’s.

Als u het vermoeden heeft dat uw organisatie slachtoffer is geworden van een phishing aanval is het zaak om adequaat te reageren. Denk aan de volgende actiepunten:

- Blokkeer de gecompromitteerde accounts en reset de wachtwoorden.
- Blokkeer de URL / het domein van waar de phishing e-mails verstuurd zijn.
- Onderzoek[7] waarvoor de aanvaller de gecompromitteerde accounts heeft gebruikt.
    - Is er spam verstuurd?
    - Zijn er specifieke mails verstuurd met gevoelige gegevens?
    - Is het account gebruikt om verder het netwerk in te dringen?
- Is er sprake van een datalek? Moet de Autoriteit Persoonsgegevens en / of moeten betrokkenen geïnformeerd worden?
- Is het incident te herleiden tot een specifieke phishing campagne? Deel de kenmerken met Z-CERT.
- Tref maatregelen om het incident in de toekomst te voorkomen

6 https://content.fireeye.com/m-trends/rpt-m-trends-2019

7 Hulp nodig bij onderzoek? In veel gevallen kan Z-CERT u bijstaan.