Vergissen is menselijk, ook bij het intypen van een e-mailadres. Maar door dit soort vergissingen kan gevoelige informatie eenvoudig in onbevoegde handen geraken. De investering voor kwaadwillenden om dergelijke informatie te bemachtigen hoeft namelijk niet meer dan tien euro te bedragen. Gelukkig kan een organisatie zich net zo makkelijk tegen deze dreiging wapenen. Maar dat moet dan wel even gebeuren...

tekst Johri Maat & Francisco Dominguez Santos

Spioneren voor een tientje

De term 'Typosquatting' is een samentrekking van 'typo' (typefout) en 'squatting' (zich illegaal vestigen, kraken). Bij typosquatting maakt men gebruik van het gegeven dat gebruikers van internet en e-mail soms fouten maken. Voorbeelden hiervan zijn het overslaan of verwisselen van letters in de domeinnaam (bijv. *minbkz.nl* i.p.v. *minbzk.nl*), vergissingen in de benaming van het domeinnaam (bijv. *ministeriebzk.nl* i.p.v. *minbzk.nl*) of een verkeerd top level domain (bijv. *minbzk.org* i.p.v. *minbzk.nl*).

E-MAIL

Een kwaadwillende maakt hier misbruik van door een website op te zetten of een *catch all* e-mailserver te maken met een vrijwel gelijke ('lookalike') domeinnaam als de organisatie die men op het oog heeft. Alle internet- en e-mailgebruikers die dezelfde typefout of vergissing maken, komen met hun browser terecht op de website of met het e-mailbericht in de inbox van de 'typosquatter'.

De populariteit van een bonafide website wordt bij typosquatting misbruikt om bezoekers te trekken. Het kan bijvoorbeeld gaan om een gok- of pornosite, een site van een concurrent of een nagebootste internetpagina. Hiermee kan een kwaadwillende bijvoorbeeld toegangs- of creditcardgegevens ontfutselen (*phishing*) of de organisatie van de originele website bekritiseren of bespotten (bijvoorbeeld door activisten).

Bij e-mailverkeer kan men door middel van typosquatting berichten ontvangen die niet voor de ontvanger zijn bestemd. Alle e-mailberichten die eindigen op de domeinnaam komen op de e-mailserver binnen. Niet alle op deze wijze ontvangen e-mailberichten zullen even interessant of relevant zijn, maar de kosten en inspanningen zijn zeer gering en de kans dat er iets interessants tussen zit is reëel. In deze bijdrage wordt verder ingegaan op typosquatting gericht op e-mailverkeer.

VORMEN VAN MISBRUIK

Wanneer men zich alleen richt op het ontvangen en meelezen van de e-mailberichten wordt dit passieve typosquatting genoemd. Wanneer men de ontvangen informatie gebruikt voor social engineering of een 'Man In The MailBox' (MITMB) aanval wordt dit actieve typosquatting genoemd.

Social engineering aanvallen bestaan uit het manipuleren van een persoon om gevoelige informatie te bemachtigen of acties uit te laten voeren die normaliter niet zouden worden gedaan. Dergelijke aanvallen kunnen zowel fysiek als digitaal worden uitgevoerd. Hierbij wordt vaak gebruik gemaakt van het feit dat mensen graag behulpzaam willen zijn. De digitale aanvallen vinden vaak plaats met behulp van e-mail, waarbij het doel is om de gebruiker te infecteren met kwaadaardige software of om gevoelige informatie

te achterhalen. Het doel van de social engineering aanval is om het slachtoffer over te halen om het e-mailbericht te openen zodat het slachtoffer kan worden geïnfecteerd. Dit kan bijvoorbeeld plaatsvinden met een bijlage maar ook door middel van een URL waar het slachtoffer op klikt. Zodra de gebruiker klikt probeert de website misbruik te maken van eventuele kwetsbaarheden in de browser of software van derde partijen om op die manier de gebruiker te infecteren.

Bij een Man In The MailBox' (MITMB) aanval stelt de aanvaller zichzelf op als een 'doorgeefluik'. Hierdoor kan een aanvaller langer onopgemerkt blijven. Tevens kan een aanvaller de berichten aanpassen voordat hij deze doorgeeft. Op deze wijze is het mogelijk om meer informatie te achterhalen of juist minder of foutieve informatie door te geven.
Doordat in veel e-mailprogramma's de eenmaal ingetypte adressen automatisch worden opgeslagen, merkt de verzender niet meer dat een verkeerde domeinnaam wordt gebruikt. Ook het gebruik van de reply all mogelijkheid maakt dat het e-mailadres met de verkeerde domeinnaam steeds verder verspreid raakt. Het feit dat veel gebruikers van e-mail aannemen dat geen bericht goed bericht is, zorgt ervoor dat deze aanval onopgemerkt kan plaatsvinden. Bij het versturen van e-mailberichten gaat het bijna altijd goed en in die gevallen dat het e-mailadres niet bestaat of de inbox vol is krijgt de verstuurder van het bericht daar een melding van. Bij een typosquatting aanval wordt alle ontvangen e-mail verwerkt maar wordt de verzender hier niet van op de hoogte gesteld. Hierdoor nemen de slachtoffers vaak aan dat het verstuurde e-mailbericht correct is aangekomen. Pas wanneer de verzender zelf om een reactie vraagt en deze niet krijgt, zal de verzender proberen te achterhalen waar het is misgegaan of in veel gevallen hetzelfde e-mailbericht opnieuw versturen.

Typosquatting is een laagdrempelige, goedkope - een domein is te registreren voor minder dan tien euro - en interessante methode voor inlichtingendiensten, journalisten en activisten.

PRAKTIJKTEST

Tot zover 'de theorie'. In het kader van bewustwording en risicoanalyse is onderzocht in hoeverre het domein '*minbzk.nl*' van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) gevoelig was voor typosquatting. Hiertoe werd door het IT-beveiligingsbedrijf Fox-IT in samenwerking met het ministerie van BZK het destijds nog vrij beschikbare domein '*minbkz.nl*' geregistreerd en werden alle binnenkomende berichten verzameld.

→ In een periode van achttien weken kwamen op het domein '*minbkz.nl*' 271 e-mailberichten binnen. Gedurende de test ontvingen de afzenders geen reactie. Op deze wijze werd dezelfde situatie nagebootst als wanneer een malafide partij het domein in beheer zou hebben.
De ontvangen berichten zijn alleen geanalyseerd op type inhoud en afzender. De informatie zelf is met het oog op de privacy verder niet gebruikt. Na afloop van de test hebben alle afzenders mede in het kader van bewustwording een waarschuwingsbericht met toelichting ontvangen en zijn de e-mailberichten vernietigd. Ook is het domein '*minbkz.nl*' juridisch overgedragen aan de Rijksoverheid en is tevens een aantal andere voor de hand liggende 'lookalike' domeinen van het ministerie geregistreerd.

RESULTATEN

De afzenders bestonden uit medewerkers van het ministerie die zichzelf vanaf een privé e-mailadres mailden, medewerkers die vanuit het eigen '*minbzk.nl*' domein een andere medewerker wilden mailen en derden (burgers, bedrijven en andere overheden) die een medewerker wilden mailen.
De ontvangen berichten waren onder meer in te delen als afspraakverzoeken, beleidsinhoudelijke zaken, facilitaire zaken, nieuwsbrieven en uitnodigingen, privé-communicatie en sollicitaties. Met name de 'beleidsinhoudelijke zaken' bevatte informatie die men alleen al vanwege mogelijk imagoschade niet graag in verkeerde handen ziet. Bij een beperkt aantal was er zelfs sprake van een concreet afbreukrisico door de mogelijke compromittering van operationele informatie en politiek gevoelige dossiers. Maar ook de informatie uit de categorieën 'afspraakverzoeken' en 'facilitaire zaken' kon door kwaadwillenden worden misbruikt, bijvoorbeeld voor social engineering. Zo kan een kwaadwillende een storingsmelding gebruiken om zich als storingsmonteur voor te doen en zo een organisatie binnen te dringen.

Deze praktijktest toonde aan dat typosquatting niet alleen een theoretisch risico is. Het rechtvaardigt dan ook dat door organisaties maatregelen worden getroffen om dit risico beheersbaar te maken.

MAATREGELEN

Om de kwetsbaarheden van typosquatting beheersbaar te maken zijn diverse maatregelen te treffen.
De belangrijkste maatregel is het als organisatie zelf registreren van 'lookalike' domeinen. Hierbij moet

Typosquatting is niet alleen een theoretisch risico

wel een afweging worden gemaakt tussen de waarschijnlijkheid dat iemand deze vergissing maakt en de ernst van het risico. De kosten van het registreren van deze domeinen zijn overigens verwaarloosbaar.
In de ICT-infrastructuur kunnen ook diverse maatregelen worden genomen om het risico van typosquatting beheersbaar te krijgen. De belangrijkste technische maatregel bestaat uit het instellen van de e-mailserver zodat het verzenden van e-mailberichten naar 'lookalike' domeinen vanuit de organisatie niet mogelijk is. Hiermee wordt in ieder geval voorkomen dat medewerkers onderling per abuis een e-mailbericht naar een 'lookalike' domein zenden. Tevens zouden sectorbreed afspraken kunnen worden gemaakt over elkaars (door derden geregistreerde) 'lookalike' domeinen. Ook kan worden besloten om informatie vanaf een bepaald classificatieniveau altijd versleuteld te versturen. Hiermee worden de gevolgen van een 'typosquatting' aanval beperkt, aangezien de aanvaller geen toegang tot de verkregen informatie heeft.
Ook kunnen de adresboeken van de medewerkeraccounts automatisch op 'lookalike' adressen worden doorzocht, waarna deze bijvoorbeeld kunnen worden geblokkeerd.
Voorlichting over typosquatting zou verder een onderdeel van de interne bewustwordingsactiviteiten op het terrein van informatiebeveiliging moeten zijn. Maar de voorlichting kan zich ook richten op derden, zoals de verzenders naar deze domeinnamen een waarschuwingsbericht te zenden.

AFSLUITING

Typosquatting vormt een reële dreiging voor organisaties. Maar deze dreiging is relatief eenvoudig en tegen lage kosten beheersbaar te krijgen. Gewoon een kwestie van doen, voordat een ander je voor is. ■

mr. J.H. Maat MSSM is senior adviseur bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
F. Dominguez Santos is senior IT security expert bij Fox-IT