Compleon
CYBERSECURITY & COMPLIANCE

De Hofstede 30
4033 BV Lienden
www.compleon.nl
info@compleon.nl
+31 (0) 85 0 70 85 20

KvK: 93505361
BTW: NL005024334B42
IBAN: NL93 KNAB 0775 3904 29

Preventieve maatregelen voor het beperken van gevolgen van phishing

Door: Rijk Prosman
Datum: 25 november 2025

AANLEIDING

Phishing vormt een van de grootste digitale bedreigingen voor organisaties, ongeacht hun omvang of sector. Omdat cybercriminelen steeds slimmer te werk gaan, is het cruciaal dat medewerkers alert blijven op verdachte berichten en links. Het vergroten van bewustzijn binnen de organisatie is hierbij geen luxe, maar een noodzaak. Praktische phishingsimulaties, mits zorgvuldig toegepast, blijken een doeltreffend hulpmiddel om medewerkers te trainen en hun weerbaarheid te vergroten. Toch is het - zeker binnen grote organisaties - onrealistisch om te verwachten dat niemand ooit op een phishingmail klikt. Dit betekent dat het risico op schade altijd aanwezig blijft. Juist daarom zijn preventieve maatregelen onmisbaar: ze beperken de mogelijke schade en beschermen zo de continuïteit van de organisatie.

In dit document worden de belangrijkste preventieve maatregelen benoemd om organisaties tegen (de gevolgen van) phishing te beschermen. Ongetwijfeld zijn er nog andere waardevolle maatregelen die hier niet aan bod komen. Suggesties en aanvullingen zijn dan ook van harte welkom en kunnen worden gedeeld via info@compleon.nl.

MAATREGEL 1: BEGRIJPELIJKE MELDPROCEDURE VOOR INCIDENTEN

Het is van cruciaal belang dat medewerkers precies weten hoe en waar zij een securityincident moeten melden. Vaak denken mensen dat als ze per ongeluk op een phishinglink klikken en er niet direct iets opvallends gebeurt, ze dit niet hoeven te rapporteren. Toch is het juist wél belangrijk om ook deze ogenschijnlijk onschuldige situaties te melden, hoe klein het incident ook lijkt. Daarmee kan de organisatie snel ingrijpen en mogelijke schade of verdere verspreiding voorkomen. Ook als je twijfelt, is het altijd beter om het incident even door te geven—zo houden we samen de digitale veiligheid op peil.

MAATREGEL 2: VEILIGE CULTUUR VOOR HET MELDEN VAN INCIDENT

Medewerkers ervaren vaak schaamte of het gevoel dat ze dom zijn wanneer ze per ongeluk op een phishinglink klikken. Het is belangrijk om te benadrukken dat zelfs de meest ervaren collega's dit kan overkomen. Niemand is altijd alert, en fouten maken hoort bij het leerproces. In plaats van uitgelachen te worden of voor gek verklaard, verdienen medewerkers een compliment als ze het lef tonen om hun fout te melden. Zo creëren we samen een open en veilige omgeving waarin iedereen zich gesteund voelt om incidenten te rapporteren, ongeacht de oorzaak.

MAATREGEL 3: ZORG VOOR EEN WERKPROCEDURE DIE CORRECTE BEHANDELING BORGT

Wanneer een medewerker op een phishinglink heeft geklikt, is het van groot belang dat er een duidelijke werkprocedure beschikbaar is waarin stap voor stap staat beschreven welke acties ondernomen moeten worden. Deze procedure moet altijd op dezelfde manier gevolgd worden, ongeacht wie het incident behandelt, zodat je zeker weet dat er geen stappen worden overgeslagen. Het bijhouden van een checklist, die bij het incident wordt opgeslagen, zorgt ervoor dat je achteraf altijd kunt terugzien welke handelingen zijn uitgevoerd. Besteed je deze taken uit aan een externe ICT-leverancier, leg dit dan goed vast, bijvoorbeeld in het Dossier Afspraken en Procedures (DAP). Deze aanpak geldt niet alleen voor phishingincidenten, maar dit is ook van belang bij andere veel voorkomende incidenten.

MAATREGEL 4: GEAVANCEERDE E-MAILBEVEILIGING

Maak gebruik van geavanceerde e-mailbeveiliging om phishingrisico's verder te beperken. Microsoft 365 biedt bijvoorbeeld de module Defender for Office 365, die standaard onderdeel is van Microsoft Business Premium. Deze oplossing scant inkomende e-mails op een slimme manier en bevat functionaliteiten zoals SafeLinks, waarbij links in e-mails extra worden gecontroleerd op schadelijkheid zodra erop geklikt wordt, en Safe Attachments, waarbij bijlagen eerst in een beveiligde omgeving worden geanalyseerd voordat ze toegankelijk zijn voor de gebruiker. Daarnaast is het mogelijk om personen binnen de organisatie die kwetsbaarder zijn voor CEO-fraude of gerichte aanvallen, extra te beschermen met aanvullende instellingen.

MAATREGEL 5: BEVEILIG DOMEINNAMEN MET EEN GOEDE SPF, DKIM EN DMARC CONFIGURATIE

Het toepassen van hardening op domeinnamen is van belang om er voor te zorgen dat domeinnamen niet misbruikt worden. Zo voorkom je door het correct instellen van **SPF**, **DKIM** en **DMARC** misbruik zoals phishing en spoofing. Dit geldt niet alleen voor domeinnamen die actief worden gebruikt, maar **ook voor domeinnamen die enkel zijn geregistreerd** en niet worden gebruikt voor de hosting van een website of het gebruik van e-mail. Zonder deze beveiliging kunnen dergelijke domeinen namelijk eenvoudig worden misbruikt voor phishing.

> **SPF** staat voor **Sender Policy Framework**, is een veiligheidsmaatregel voor e-mails. Het controleert of een e-mail echt van de afzender komt door te controleren of de server die de e-mail verzendt, is geautoriseerd. Het juiste gebruik van SPF helpt om te voorkomen dat uw domeinnaam wordt misbruikt door hackers voor phishingdoeleinden.
>
> **DKIM** staat voor **Domain Keys Identified Mail**. E-mailberichten worden voorzien van een digitale handtekening, die de ontvanger kan controleren. Zoals ook het geval is bij SPF, helpt DKIM om te voorkomen dat uw domeinnaam wordt misbruikt door hackers voor phishingdoeleinden.
>
> **DMARC** staat voor **Domain-based Message Authentication, Reporting & Conformance**. Domeinnaamhouders kunnen via DMARC instellen hoe strak het beleid van SPF en DKIM moet worden opgevolgd door ontvangers. Net zoals bij SPF en DKIM helpt DMARC om te voorkomen dat uw domeinnaam wordt misbruikt door hackers voor phishingdoeleinden.
>
> > ***Let op!*** *Voor een streng DMARC-beleid moeten alle systemen die e-mail versturen namens uw domein correct zijn ingesteld met SPF of DKIM. Als dat niet zo is, kunnen ook legitieme e-mails worden geweigerd.*

MAATREGEL 6: 100% MULTIFACTORAUTHENTICATIE (MFA)

Invoeren van MFA voor alle gebruikers

Het invoeren van multifactorauthenticatie (MFA) is een van de meest effectieve maatregelen tegen ongeautoriseerde toegang. MFA vereist dat medewerkers zich naast hun wachtwoord met een tweede factor identificeren, zoals een authenticator-app of hardware-token. Hierdoor voorkomt MFA dat aanvallers kunnen inloggen met buitgemaakte wachtwoorden, bijvoorbeeld na phishing of een datalek.

Stel MFA verplicht voor alle accounts, niet alleen voor beheerders, en ondersteun medewerkers bij de inrichting ervan. Dit is essentieel omdat criminelen bij Business Email Compromise (BEC) vaak de mailbox van een medewerker overnemen en vanuit dat legitieme adres overtuigende fraudeberichten versturen. Wanneer MFA verplicht is, kunnen aanvallers - zelfs met een correct wachtwoord - niet zomaar toegang krijgen tot een mailbox.

Gebruik phishing-resistente vormen van MFA

Niet elke vorm van MFA is even veilig. Pushmeldingen, SMS-codes of authenticator-apps zijn beter dan alleen een wachtwoord, maar kunnen soms worden misleid via geavanceerde phishing. Overweeg daarom moderne opties zoals FIDO2-sleutels, passkeys of Windows Hello, die technisch onmogelijk zijn te phishen. Deze oplossingen worden onder meer door NIST en het NCSC aanbevolen.

Conditional Access (Microsoft 365)

Om MFA organisatiebreed af te dwingen, zowel voor eigen gebruikers, als ook voor gastaccounts, is het aanbevolen om hiervoor Conditional Access te gebruiken. Daarnaast is het mogelijk om via Conditional Access oude en onveilige protocollen te blokkeren en toegang te weigeren vanaf risicovolle locaties. Hiermee wordt het voor aanvallers nóg moeilijker om toegang te krijgen, zelfs als zij beschikken over inloggegevens.

MAATREGEL 7: ENDPOINT PROTECTION MET DE JUISTE INRICHTING EN OPVOLGING

Inrichting

Een goede oplossing voor Endpoint Protection is vaak het laatste vangnet wanneer een medewerker op een phishinglink klikt. Aanvallers proberen na zo'n klik vaak het apparaat zelf te misbruiken. Bijvoorbeeld via schadelijke scripts, downloaders of het stelen van tokens. Een goede Endpoint Protection, kan het verschil maken dat een menselijke fout niet direct leidt tot een groter incident.

Monitoring

In veel organisaties wordt gebruik gemaakt van Microsoft 365. Microsoft Defender for Business (onderdeel van Business Premium) biedt geavanceerde functies om aanvallen te detecteren. Daarmee is deze oplossing in veel gevallen toereikend voor het MKB. Het is echter belangrijk om te benadrukken dat deze oplossing bij de activatie van het abonnement, **niet automatisch veilig is** geconfigureerd. Denk hierbij aan het activeren van de benodigde beveiligingsprofielen, het correct configureren van Defender-notificaties, het instellen van webfiltering en het afdwingen van beveiligingsbeleid via Intune of vergelijkbare oplossingen. Zonder deze configuraties blijven essentiële onderdelen uitgeschakeld en blijven apparaten kwetsbaar. De beveiliging en bescherming staat of valt met de juiste inrichting.

Voor organisaties met hogere veiligheidseisen, complexe IT-omgevingen of gevoelige data zijn er geavanceerde oplossingen. Deze bieden doorgaans snellere detectie, diepgaand inzicht en betere bescherming, maar vragen meer investering en specialistisch beheer.

Opvolging

Goede opvolging cruciaal. Een melding vanuit de Endpoint Protection betekent niet automatisch dat het probleem is opgelost. Een melding moet daarom altijd worden beoordeeld of het incident vervolgacties vereist, zoals loganalyse, netwerkcontrole of het uitsluiten van verdere compromittering. Zonder structurele opvolging kunnen subtiele dreigingen onopgemerkt blijven.

MAATREGEL 8: BLOKKEREN VAN NIEUWE DOMEINNAMEN (WEBFILTERING)

Bij phishingaanvallen maken criminelen veelvuldig gebruik van nieuw geregistreerde domeinnamen. Deze domeinen zijn vaak nog onbekend bij beveiligingssystemen en worden ingezet om legitiem lijkende e-mails te versturen of gebruikers naar kwaadaardige websites te lokken. Het blokkeren van nieuwe domeinnamen is daarom een effectieve maatregel om de kans op succesvolle phishingaanvallen aanzienlijk te verkleinen. Door dergelijke domeinen standaard te blokkeren, wordt het voor aanvallers een stuk lastiger om nietsvermoedende medewerkers te misleiden.

Helaas is het binnen de Microsoft 365-omgeving niet mogelijk om automatisch het ontvangen van e-mails van nieuwe domeinnamen te blokkeren. Dit betekent dat deze maatregel niet direct toepasbaar is op inkomende e-mailverkeer binnen deze omgeving. Gelukkig zijn er binnen webfiltering in Microsoft Defender wel mogelijkheden om nieuwe domeinnamen te blokkeren. Hierdoor kan worden voorkomen dat medewerkers via phishinglinks in e-mails of chats toch op gevaarlijke websites terechtkomen. Zo vormt webfiltering een belangrijke aanvullende verdedigingslinie tegen moderne phishingaanvallen.

MAATREGEL 9: BEPERKING RECHTEN OP WERKPLEKSYSTEMEN

Het beperken van rechten van medewerkers op werkpleksystemen is een zeer effectieve maatregel om de impact van cyberdreigingen te minimaliseren. Wanneer medewerkers zonder beheerrechten werken, kan malware of schadelijke software aanzienlijk minder schade aanrichten, omdat deze geen toegang heeft tot kritieke systeeminstellingen of het installeren van ongewenste programma's. Door ervoor te zorgen dat alleen vooraf goedgekeurde software mag worden uitgevoerd, wordt de kans op het binnenhalen van ongewenste of kwaadaardige applicaties verder verkleind.

Bovendien is het verstandig om het uitvoeren van scripts te beperken door bijvoorbeeld macro's standaard te blokkeren en het gebruik van PowerShell te beperken tot alleen geautoriseerde beheerders. Op deze manier wordt het voor aanvallers een stuk lastiger om via geautomatiseerde scripts of malafide macro's systemen te compromitteren. Deze aanpak zorgt ervoor dat zelfs als een medewerker per ongeluk op een verkeerde link klikt, de potentiële schade beperkt blijft tot een minimum.

MAATREGEL 10: (MANAGED) SOC-DIENSTEN

Een Security Operations Center (SOC) is een gespecialiseerde afdeling die continu IT-systemen en netwerken bewaakt om cyberdreigingen snel te detecteren en te bestrijden. Enterprise organisaties hebben dit vaak zelf in huis of zijn aangesloten bij bekende cybersecuritybedrijven die Security Operations Center (SOC-diensten) leveren. Voor het MKB zijn deze diensten vaak onbetaalbaar. Het goede nieuws is dat steeds meer IT-bedrijven SOC-diensten aanbieden tegen betaalbare tarieven. Dat zijn niet één-op-één vergelijkbare diensten met de SOC-diensten van de bekende cybersecurity bedrijven, maar zijn wel uiterst effectief en passend voor het MKB. Enkele voorbeelden hiervan zijn RocketCyber en Huntress.

Met een SOC-dienst krijgt een organisatie 24/7 monitoring van kritische systemen en netwerken, waardoor verdachte activiteiten snel worden gesignaleerd en incidenten direct opgevolgd kunnen worden. Voor het MKB betekent dit dat men niet zelf alle expertise in huis hoeft te halen, maar kan vertrouwen op externe specialisten die proactief meekijken. Dit verkleint de kans dat een aanval of inbraak onopgemerkt blijft en zorgt ervoor dat er altijd iemand paraat staat om adequaat te reageren als het misgaat. Zo kunnen zelfs kleinere organisaties zich goed wapenen tegen geavanceerde cyberdreigingen, zonder dat ze het wiel zelf hoeven uit te vinden.