School CERT

Phishing

Hulp bij een phishingaanval

Bij een phishingaanval proberen cybercriminelen persoonlijke gegevens of wachtwoorden te stelen. Ze doen dit door naar een valse website te lokken of door je te vragen je persoonlijke gegevens door te geven. Phishingmails lijken altijd afkomstig van een betrouwbare partij, zoals een bank, ict-leverancier of verzekeraar. Ook CEO-fraude komt regelmatig voor. Hierbij lijkt de mail afkomstig van de directeur van een bedrijf.
Ondanks getroffen maatregelen kan het gebeuren dat een phishingpoging succesvol is en een aanvaller inloggegevens buitmaakt. Met een gestructureerde aanpak kun je de impact van een gelukte phishingpoging minimaliseren, zodat de veiligheid van de school intact blijft.

Heb je een melding van phishing ontvangen of heb je een sterk vermoeden van phishing? Dit document geeft je de handvatten om hier op de juiste manier mee om te gaan.

Stappenplan

1. Identificatie en analyse

Analyseer de phishingmail

Analyseer de gerapporteerde phishingmail en stel vast dat het om een phishingmail gaat.
Open geen phishingmail op een apparaat met toegang tot gevoelige gegevens, aangezien het bericht mogelijk malware bevat.

Een phishingmail bevat een aantal kenmerken die indicators of compromise (IOC's) worden genoemd. Verzamel onderstaande IOC's van de phishingmail die van belang zijn voor verder onderzoek:
- Afzender.
- Onderwerp.
- Url's en domeinnamen (klik niet op url's/links, maar open ze via online tools: virustotal, urlscan of urlvoid).
- Bijlage.
- Inhoud van de mail.

Bepaal scope

Je kunt hierbij de volgende vragen stellen om de ernst en type dreiging te bepalen:
- Naar wie is de mail gestuurd?
- Op basis van het afzender adres en/of onderwerp van de mail kan uitgezocht worden naar wie de mail gestuurd is. Vraag de beheerder van je mailserver om dit te doen.
    - Is het gericht aan een specifiek persoon bijvoorbeeld schoolbestuurder of aan een afdeling?
- Wat is het doel van de phishing?
    - Het verzamelen van inloggegevens.
    - Het verspreiden van malware.

Bepaal de impact

- Welke gebruikers hebben de url bezocht?

- Vaak wordt er bij een phishingmail gebruik gemaakt van een url. Op basis van bijvoorbeeld proxy logging, firewall logging of logging van Endpoint Detection & Response (EDR) kan gecontroleerd worden wie de url uit de phishingmail hebben bezocht.
- Vraag de gebruikers of ze de bijlage hebben geopend of credentials hebben achtergelaten.
- Is multifactor-authenticatie geactiveerd voor het account?
- De impact van het achterlaten van inloggegevens wordt beperkt door gebruik van multifactor-authenticatie (MFA). Er is dan naast het wachtwoord nog een extra authenticatiestap. Ga na of de gebruiker deze extra authenticatiestap ook heeft uitgevoerd.

Registratie

- Registreer het incident en bepaal de prioriteit.
- Leg de resultaten, de acties en besluitvorming vast in een logboek of incidentregistratiesysteem.

2. Containment

Stop verdere verspreiding

- Stel de e-mail veilig voor verder onderzoek door deze op te slaan, bijvoorbeeld in een met wachtwoord beveiligd zip-bestand.
- Zorg ervoor dat de mail niet verder verspreid of geopend kan worden. Verwijder de e-mail uit de mailbox van de getroffen gebruikers of informeer de getroffen gebruikers (zowel intern als extern) over de phishingmail en vraag ze de mail te verwijderen.
- Blokkeer de phishingcampagne door de afzender, url, domeinnamen en de bijlage te blokkeren op de mailvoorziening. De beheerder van de mailvoorziening kan dit doen. Veel endpoint protectionsystemen, zoals Microsoft Defender for Endpoint, bieden de mogelijkheid voor het blokkeren van url's, domeinnamen, en bestanden op basis van filehashes. Dit kan door de beheerder van de endpoint protectionsysteem worden uitgevoerd.

Blokkeer accounts en wijzig wachtwoorden

- Blokkeer externe toegang en wijzig het wachtwoord van alle accounts waarvan de gegevens zijn achtergelaten op de phishingsite of die de bijlage hebben geopend.
- Laat de ict-beheerder alle actieve sessies beëindigen van de getroffen account(s).
- Wijzig de wachtwoorden op een computer waarvan zeker is dat deze niet geïnfecteerd is met malware. Wachtwoorden worden vaak hergebruikt. Wijzig daarom het wachtwoord voor alle accounts waarbij dit wachtwoord gebruikt is.

Isoleer de computer

- Als je vermoedt dat er sprake is van een malware-infectie, laat de computer dan aan staan. Dit in verband met mogelijke sporen en aanwijzingen voor digitaal forensisch onderzoek.
- Verbreek de netwerkverbinding van de computer. Zo zorg je ervoor dat hackers niet meer bij de computer kunnen en dat de malware zich niet kan verspreiden in het netwerk.

3. Onderzoek

Voer een grondig onderzoek uit naar de oorsprong van de mail:

- Email artifacts: afzender, onderwerp, body van de mail, e-mail header.
- Url's/domeinnamen, DNS-register, hostingpartij, broncode van de phishing site.
- Analiseer attachment via sandboxingtools en verzamel IOC's.
- Controleer of url's, domeinnamen, filehashes bekend zijn op verschillende threatintelligence services zoals virustotal.

Controleer inlogpogingen:

- Zijn er inlogactiviteiten vanaf ongebruikelijke locaties, systemen, user-agents of op afwijkende tijdstippen voor de accounts waarvan gegevens zijn achtergelaten?
- Is er succesvol ingelogd vanaf het betreffende ip-adres? Zo ja, dan is het account gecompromitteerd.
- Is er ook succesvol ingelogd vanaf het betreffende ip-adres met andere accounts die nog niet in scope waren van het onderzoek? Zo ja, blokkeer ook deze accounts.

Onderzoek waarvoor de aanvaller de gecompromitteerde accounts heeft gebruikt:

- Is er spam verstuurd?
- Zijn er specifieke mails verstuurd met gevoelige gegevens?
- Worden binnenkomende e-mails doorgestuurd of naar de prullenbak gestuurd?
- Stel vast welke rechten de gebruiker had in de mailomgeving en controleer op malafide wijzigingen. Bijvoorbeeld: als een gebruiker rechten had om mensen toe te voegen aan bepaalde distributielijsten, controleer dan of er recente wijzigingen zijn geweest op dat vlak.
- Voer de bovenstaande stappen ook uit voor andere mailboxen waartoe deze gebruiker toegang had. Ook voor shared mailboxen kan je forwards instellen.
- Controleer of de contactgegevens van de getroffen gebruiker nog kloppen in het mailsysteem (telefoon, adres etc).

4. Herstel

Herstel accounts

- Stel na afloop van het onderzoek vast welke accounts getroffen zijn. Mogelijk zijn er meer accounts getroffen dan in eerste instantie (stap 2) werd aangenomen. Reset de accounts en wijzig de wachtwoorden van alle getroffen accounts.
- Verwijder eventueel aangemaakte forwarding- en inboxrules van de mailbox. Voeg het e-mailadres waarnaar de mail is doorgestuurd toe aan de blocklist op de e-mailvoorziening.
- Herstel de contactgegevens van de getroffen gebruiker in het mailsysteem (telefoon, adres etc).
- Herstel de rechten van de gebruiker in de mailomgeving en verwijder malafide wijzigingen.
- Activeer multifactor-authenticatie indien dit nog niet geactiveerd is.

Opschonen systemen

Als er malafide software is geïnstalleerd, verwijder deze dan met malware-verwijdertools, bijvoorbeeld Malwarebytes of Bitdefender. Nog beter is om het systeem opnieuw in te richten. Laat de gebruiker het wachtwoord wijzigen van al zijn accounts.

Communicatie

Als er mail gestuurd is vanuit het getroffen account, informeer dan de privacy officer en/of functionaris gegevensbeschermer (FG) van je organisatie. Bepaal samen of er sprake is van een datalek en of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Doe dit in de eerste 72 uur na ontdekking van het datalek.

Informeer proactief eventuele betrokkenen – bijvoorbeeld ouders, leerlingen en/of medewerkers– over de aanval, de genomen maatregelen en eventuele stappen die zij moeten ondernemen.

5. Rapportage en evaluatie

Rapporteer het incident en de genomen maatregelen aan het management en/of het schoolbestuur. Evalueer de effectiviteit en tijdigheid van de respons om toekomstige reacties mogelijk te verbeteren.

Preventieve maatregelen

Identificeer zwakke punten in het beveiligingsproces en implementeer verbeteringen om toekomstige aanvallen te voorkomen.

Verdieping

Meer informatie over hoe te beschermen tegen phishing is te vinden in:

- Phishing - Aanpak informatiebeveiliging en privacy in het onderwijs (kennisnet.nl)
- Veilig omgaan met e-mail op uw school: 5 maatregelen (kennisnet.nl)
- Beveiligingsvoorschriften op edustaandaard.nl

Overzicht van tools

- Virustotal
- Urlscan
- Urlvoid
- Malwarebytes
- Bitdefender
- Hybrid Analysis
- Joe Sandbox

Laatst geupdate 02-10-2024

Voor ondersteuning: support@kennisnet.nl / 0800 321 22 33
Voor vragen over het School-CERT: cert@kennisnet.nl