Definitieve versie september 2024

Protocol Cybercriminaliteit

rentree. thuis in Deventer

Procedure:

BO besluit d.d. 5 september 2024

Inhoud

1 Inleiding & aanleiding

ICT vervult een prominente rol in het dagelijks leven, voor het ondersteunen van bedrijfsprocessen en bij het bedienen van allerlei complexe processen in vitale infrastructuren. ICT is diep ingebed in de samenleving. Vandaag de dag bewaren we al onze gegevens en kennis ergens elektronisch en zijn we aangewezen op de beschikbaarheid en integriteit van computersystemen en telecommunicatienetwerken. Helaas kennen we ook een andere kant, waarbij ICT-middelen worden misbruikt of ingezet voor illegale activiteiten. Dit misbruik wordt ook wel cybercriminaliteit of cybercrime genoemd.

Bij cybercriminaliteit denken veel mensen aan jonge hackers die voor de lol of vanuit een ideologie de website van een bedrijf kraken. Maar er zijn ook criminele bendes die er op uit zijn om geld te ontfutselen. Voorbeelden van cybercrime zijn het 'gijzelen' van gegevens op een computer (ransomware), het zogenaamd bellen namens een IT-bedrijf (Microsoft (tech) scam), het kopiëren van de chip op een bankpas of het verspreiden van kwaadaardige software om internetbankieren te manipuleren.

1.1 Rentree

Ook Rentree is kwetsbaar, getuige de virusmelding met ransomware van 01-11-2016. De ervaringen van onder andere deze aanval zijn vertaald in onderliggend handelingsprotocol voor gebruik tijdens eventueel toekomstige bedreigingen. Dit naast en als aanvulling op de maatregelen die in het verleden al zijn genomen in samenwerking met de ICT-partners / dienstverleningspartners van Rentree.

1.2 Cybercriminaliteit

Norea[1] omschrijft cyberciminaliteit als: criminaliteit gepleegd via computers en/of ICT-netwerken. Of anders geformuleerd: criminaliteitsvormen waarbij ICT een wezenlijke rol speelt.

Volgens het NCSC[2] zijn er een aantal verschijningsvormen waaraan cybercriminaliteit / handelingen ingedeeld kunnen worden:

Verschijningsvorm	Omschrijving / toelichting
Malware	Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse *malicious software* (kwaadaardige software, soms schadelijke software). Malware veronderstelt kwade opzet.
Computerinbraak (hacking)	Het zonder toestemming een computernetwerk binnendringen door de beveiliging te kraken. Niet altijd met de bedoeling om illegaal informatie toe te eigenen, maar veelal om aan te tonen dat het netwerk onvoldoende beveiligd is. Er zijn wel hackers met criminele bedoelingen, echter, voor velen is het een sport om beveiligde netwerken te kraken
Botnets	Een collectie van aan elkaar gekoppelde computers die software gebruiken die meestal is geïnstalleerd door een computerworm,

[1] Norea is de beroepsorganisatie van IT-auditors (http://www.norea.nl/)

[2] NCSC: Nationaal Cyber Security Centrum, onderdeel van het Ministerie van Veiligheid en Justitie (https://www.ncsc.nl/)

Verschijningsvorm	Omschrijving / toelichting
	Trojaans paard of achterdeurtje. De geïnfecteerde computers heten ook wel zombies, het botnet heet ook wel zombienetwerk.
Website aanvallen/ Denial of Service-aanvallen (DoS, DDoS)	Pogingen om een computer, computernetwerk of dienst onbeschikbaar te maken voor de bedoelde gebruiker. Het verschil tussen een 'gewone' dos-aanval en een distributed dos-aanval is dat meerdere computers tegelijk de aanval uitvoeren naar hun doelwit
Social engineering	Een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen. Dit door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. De aanval is gericht op het verkrijgen van vertrouwelijke of geheime informatie, waarmee de hacker dichter bij het aan te vallen object kan komen.
E-mailgerelateerde verschijningsvormen (phishing, virus)	Bijvoorbeeld phishing / hengelen: Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank. De meeste vormen van phishing gebeuren via e-mail. De slachtoffers worden hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren". Een variante vorm van phishing is spear fishing, waarbij de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer worden gebruikt om hem een gevoel van vertrouwen te geven Een computervirus (in het dagelijks taalgebruik wordt meestal kortweg over virus gesproken) is een vorm van schadelijke software (malware). Het is een computerprogramma dat zich in een bestand kan nestelen, bijvoorbeeld in bestanden van een besturingssysteem. Computervirussen worden als schadelijk beschouwd omdat ze schijfruimte en computertijd in beslag nemen van de besmette computers. In ernstige gevallen kunnen virussen binnenin de computer schade aanrichten, bijvoorbeeld het wissen en verspreiden van gevoelige gegevens. In zeer ernstige gevallen kan de gebruiker zelfs de totale controle over de computer verliezen.

Vaak komen de verschillende vormen voor in combinatie met andere technieken. Zo kan een computervirus dienen om een Trojaans paard te verspreiden, dat gegevens steelt tijdens een criminele activiteit. Ook kan eerst een netwerk worden afgeluisterd om vervolgens met de verkregen gegevens een ander computersysteem binnen te dringen.

Een ander onderscheid wordt gemaakt tussen gerichte en ongerichte cyberaanvallen. Ongerichte cyberaanvallen hebben geen specifiek bedrijf of computersysteem als doelwit. Bij ongerichte aanvallen wordt getest op het bestaan van specifieke kwetsbaarheden waarna wordt getracht de kwetsbaarheid van het computersysteem te misbruiken, bijvoorbeeld door malware te installeren.

2 Omgang met Cybercriminaliteit

Rentree heeft haar technische infrastructuur uitbesteedt aan een ISO27001[3]-gecertificeerde dienstverlener[4] op basis van het concept “ontzorgen”. Daarbij is een groot deel van de technische beheersmaatregelen (zowel defensief als correctief) belegd bij een daartoe gespecialiseerde organisatie. Dit neemt niet weg dat de bedreiging van beveiligingsinbraken op het gebied van ICT niet 100% zijn weg te nemen. Niet bij de dienstverlener en niet bij Rentree zelf.

Een groot deel van de kwetsbaarheid is gelegen in de zogenaamde “social engineering”-aspecten, waarbij een gebruiker verleidt wordt om bestanden met virussen te downloaden of openen, verwijzingen naar malafide sites aan te klikken etc.

- In de bestrijding van cybercriminaliteit zijn verschillen scenario’s met eigen maatregelen mogelijk: Offensief – actieve bestrijding van cybercriminaliteit door opsporingsdiensten (bijvoorbeeld door het Team High Tech Crime van de Nederlandse politie, Interpol, anti-virus-leveranciers, etc). Hier liggen geen acties bij Rentree, buiten eventuele aangifte van incidenten;
- Defensief – pro-actieve monitoring in de vorm van technische beveiligingsmaatregelen. Hier liggen met name acties bij de dienstverlener in de vorm van virusdetectiesystemen, systeembeveiligingslagen etc);
- Correctief – reactieve maatregelen om in geval van cybercriminaliteit de bron en effecten te bestrijden (hier liggen met name acties bij de dienstverlener in de vorm van bestanden isoleren, kopieën terug te zetten of aanscherping van filtering en digitale toegangsbeveiliging);
- Preventief – pro-actieve maatregelen in de vorm van communicatie naar medewerkers om de bewustwording en kennis van de mogelijke bedreigingen te vergroten en de inzet van zelflerende beveiligingssoftware om patronen en gevaren te ontdekken in het netwerkverkeer.

2.1 Uitgangspunten

Afhankelijk van het type beveiligingsincident of cybercriminaliteit zullen maatregelen moeten worden getroffen. Daarbij gelden de volgende uitgangspunten voor Rentree:

- Defensieve en correctieve maatregelen als virusscanning, anti-spam etc worden uitgevoerd / zijn uitbesteedt aan dienstverleningspartner in overleg en samenwerking met ICT van Rentree. Een aantal concrete beveiligingsmaatregelen die zijn genomen, zijn:
    - Actieve werkplek security pakket van NEH. Bestaande uit:
        - Security Operations Center;
        - Geavanceerde Microsoft Beveiliging met E5 Security;
        - SafeLinks / Safe Attachements / Webcontent Filtering / Smart Screen;
        - Risk Based Conditional Access (o.a.: MFA, alleen ‘trusted devices’ , blokkering verdachte inlog pogingen etc.);
        - Defender for endpoint (o.a.: Virus en malware bescherming);
        - Credential Guard (bescherming van inloggegevens);
        - SOC/SIEM (detecteren van misbruik of aanvallen in een IT-omgeving).
    - Awareness trainingen
    - Verbindingen van werkplekken worden via beveiligde VPN-tunnels opgezet.

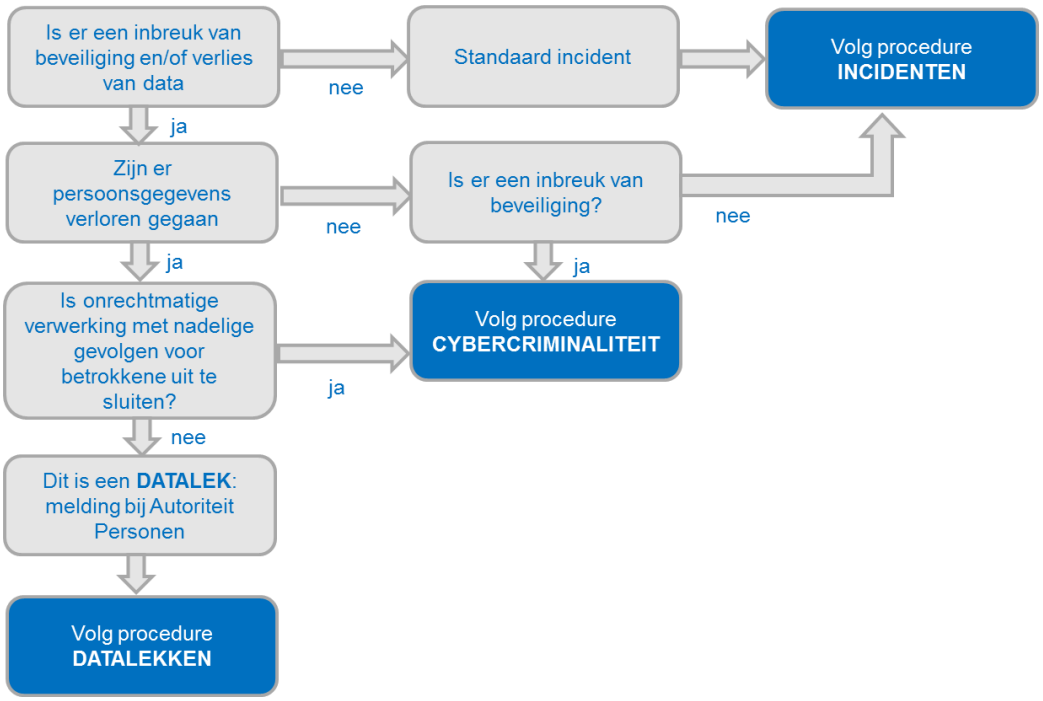
[3] ISO 27001 is een ISO standaard voor informatiebeveiliging -> https://nl.wikipedia.org/wiki/ISO/IEC_27001

[4] Dit betreft NEH Group uit Leusden

- Afhankelijk van de vorm van het beveiligingsincident en de mogelijke impact, staat Rentree een afwachtende houding voor (bijvoorbeeld: In geval Rentree getroffen wordt door ransomware of virussen, gaat Rentree in eerste instantie niet in op verzoeken tot betaling ten behoeve van vrijgeven van encryptiesleutels, tenzij dit noodzakelijk is voor de voortzetting van de bedrijfsvoering (en overige maatregelen niet voldoende effectief blijken te zijn). Dit ter inhoudelijke beoordeling door ICT en in overleg met directie.)
- Beveiligingsincidenten en bestrijding van virussen zal per inbreuk en beveiligingsincident situationeel beoordeeld worden in verband met de verschillende varianten & mogelijke consequenties (bijvoorbeeld datalekken).

2.2 Afweging vooraf

In het geval er een incident wordt geconstateerd, zal de volgende afweging worden gemaakt:



De procedure met betrekking tot cybercriminaliteit is hieronder weergegeven.

2.3 Er is een incident geconstateerd met de classificatie beveiligingsincident

Ondanks alle beschermende maatregelen, zullen cybercriminaliteit of beveiligingsincidenten niet volledig uit te sluiten zijn.

2.3.1 Protocol Cybercriminaliteit

Na constatering van de bedreiging in de categorie beveiligingsincident, zullen de volgende handelingen uitgevoerd dienen te worden:

Actie	Toelichting / omschrijving	Resultaat / kenmerk Terug te vinden in:	Datum	Tijdstip (24h)	Check √ / n.v.t
Classificatie beveiligings-incident	In overleg met de dienstverleningspartner het beveiligingsincident classificeren (oorzaak, type bedreiging, mogelijke consequenties (inclusief afweging in het kader van het protocol Datalekken), beschikbare tegenmaatregelen). Classificatie: • Zeer hoog, toenemende schade inherent aan operationeel houden van ICT-systemen : toegang per direct beperken (blokkeren netwerk, evt stroomvoorziening) • Hoog, verstoring bedrijfsvoering en gevaar voor verdere besmetting of toename van schade: toegang per direct beperken, iom hostingspartner maatregelen definiëren en doorvoeren. Mogelijke scenario's: terug naar backup • Middel, geen directe verstoring bedrijfsvoering: informeren collega's, maatregelen door hostingspartner uit te voeren (correctief & preventief) • Laag: informeren collega's, maatregelen door hostingspartner uit te voeren (aanscherpen filtering & logging)	Datum tijdstip van de inbreuk en eventueel getroffen maatregelen			
Doorvoeren maatregelen	O.b.v. classificatie beperkende of correctieve maatregelen doorvoeren	Meldingshistorie klantportaal NEH & rapportage vanuit NEH			

Actie	Toelichting / omschrijving	Resultaat / kenmerk Terug te vinden in:	Datum	Tijdstip (24h)	Check √ / n.v.t
Communicatie	• Informeren van collega's over het beveiligingsincident, de genomen maatregelen en eventuele mogelijkheden ter preventie soortgelijke incidenten • Afhankelijk van type beveiligingsincident, melding bij Team High Tech Crime van de Nederlandse politie				
Evaluatie	Evaluatie van het beveiligingsincident en de genomen maatregelen				
Registratie	Indien een bedreiging zich heeft voorgedaan wordt, na het doorvoeren maatregelen ter beheersing per geval een registratie gemaakt en vastgelegd in het primaire documentmanagementsysteem (als ICT-beveiligingsincident). Deze registratie bevat de volgende onderdelen: • Wat is er gebeurd; • Welke (tegen)maatregelen zijn genomen ter beheersing; • Welke correctieve maatregelen zijn genomen; • Welke preventieve maatregelen zijn mogelijk binnen Rentree (wat kunnen collega's zelf doen, welke vervolgacties zijn nodig en welke tips zijn er voor de organisatie); • Hoe zijn de collega's geïnformeerd en geïnstrueerd.	Primair documentsysteem, ViewPoint met kenmerk beveiligingsincident			

3 Bijlagen

3.1 Bijlage: Bronnen & gerelateerde documenten

Inhoud	Verwijzing / bronnen
Algemene informatie en best practices informatiebeveiliging voor lokale overheden	https://informatiebeveiliging-gemeenten.nl/
Algemene informatie omtrent informatiebeveiliging lokale overheden (informatiebeveiligingsdienst Nederland)	www.ibdgemeenten.nl
Cybercrime, richting definitie, afbakening en positionering, 5 maart 2012	Norea (http://www.norea.nl/)
Cybercrime, van herkenning tot aangifte, januari 2012	NCSC, Ministerie van Veiligheid en Justitie (https://www.ncsc.nl/)
De Baseline Informatiebeveiliging (woning)Corporaties (BIC), een toepassingshandleiding voor NEN/ISO 27001 en 27002 voor woningcorporaties	BIC, NetwIT
Definities & beschrijvingen	Wikipedia (https://nl.wikipedia.org)