School CERT

Ransomware

Hulp bij een ransomwareaanval

Bij een ransomwareaanval versleutelt kwaadaardige software documenten, waardoor je de toegang verliest. Een andere naam voor ransomware is gijzelsoftware. De gijzeling gaat gepaard met afpersing, waarbij de kwaadwillende organisatie ontsleuteling aanbiedt tegen betaling.

Dit document biedt schoolbesturen een stappenplan om te reageren op een ransomware-infectie waarbij meerdere apparaten getroffen zijn en de besmetting zich al verder heeft verspreid over het netwerk.

Is een stap niet direct duidelijk, kijk dan verder in het document bij het hoofdstuk: Verdieping (blz. 5).

Stappenplan

1. Identificatie, classificatie en registratie

Analyseer de situatie

Wordt er losgeld geëist? Wat eisen ze en wanneer? Van welke ransomware is er sprake? Dit kan blijken uit de losgeldbrief. Wat is de impact van de ransomware en welke systemen zijn getroffen? Registreer je bevindingen. Dit kan bijvoorbeeld in je incidentregistratiesysteem of in een logboek (zie bijlage: Logboek).

Schaal op naar een crisisteam en informeer het schoolbestuur

Blijkt uit de eerste stap dat er inderdaad sprake is van een ransomwarebesmetting die meerdere accounts of systemen raakt? Neem dan contact op met je bevoegd gezag en roep je crisismanagementteam bij elkaar. Stel samen een beeld op en besluit over te nemen stappen. Denk hierbij aan het informeren van medewerkers en ouders, het opvangen van leerlingen bij verstoring van lessen etc. Breng het team periodiek bij elkaar om te beslissen over eventuele vervolgstappen. Zie bijlage: Agenda, voor een voorbeeld van de agenda van het crisisoverleg.

2. Schade beperken

Stop verdere verspreiding

Isoleer de getroffen systemen, zodat de besmetting zich niet verder over het netwerk kan verspreiden. Dus controleer de accountactiviteit en blokkeer gecompromitteerde accounts. ***Schakel de getroffen systemen niet uit***, dit maakt het lastig om verder onderzoek te doen. Stel de back-ups veilig, koppel de back-upserver los van het netwerk en stop lopende back-ups. Stel cruciale servers veilig door ze uit te schakelen.

Stel bewijsmateriaal veilig

Start met het verzamelen van informatie voor later onderzoek door de politie of forensisch onderzoekers. Denk hierbij aan loggingsdata, data van besmette servers, verdachte e-mails of andere relevante informatie.

3. Onderzoek

Neem contact op met relevante partijen buiten je organisatie

Stel anderen op de hoogte van de ransomwareaanval en de gevolgen voor je school en/of schoolbestuur. Denk hierbij aan het School-CERT, maar ook aan andere scholen of samenwerkingsverbanden waarmee jouw schoolbestuur in verbinding staat. Neem daarnaast contact op met de politie en de Autoriteit Persoonsgegevens. Heb je een cyberverzekering? Schakel dan ook met je verzekeraar. Die heeft instructies over de vervolgstappen.

Start een onderzoek naar de ransomware

Zodra de ransomware zich niet meer verder verspreidt over het netwerk, kun je verder onderzoek doen. Dit kan worden gedaan door eigen medewerkers, de ICT-leverancier of externe onderzoekers. Bijvoorbeeld van een Incident Response-bedrijf of de partij die door de verzekeraar is aangewezen. Probeer antwoord te krijgen op de volgende vragen voor mogelijke vervolgstappen:

- Hoe zijn de aanvallers binnengekomen?
- Zitten de aanvallers nog in het netwerk?
- Zijn er gegevens gestolen?
- Wordt er om losgeld gevraagd of gedreigd met publicatie van gegevens?
- Zijn de back-ups besmet of kunnen ze worden teruggeplaatst?
- Wat is de impact voor de continuïteit van het onderwijs?

4. Herstel

Controleer of er een ransomwaresleutel beschikbaar is

In sommige gevallen is er door eerder onderzoek een ransomwaresleutel beschikbaar die kan helpen om informatie weer beschikbaar te maken. Deze sleutels zijn te vinden op de website van het NoMoreRansomProject, een initiatief van Europol.

Stel een herstelplan op voor je systemen en activiteiten

Bepaal welke systemen de hoogste prioriteit krijgen en creëer een duidelijk overzicht van de verwachte hersteltijden. Het is afhankelijk van de situatie hoelang het herstel duurt. Als er een herstelsleutel of een schone back-up beschikbaar is, kan de hersteltijd enkele dagen bedragen. Wanneer het systeem volledig opnieuw moet worden opgebouwd kan dit enkele weken duren. Dan kan uitwijken naar een andere locatie noodzakelijk zijn. Indien je bedrijfscontinuïteitsmanagement hebt geregeld, kun je waarschijnlijk werken vanuit je bedrijfscontinuïteitsplan. Zorg dat je communiceert met de betrokkenen. En betrek het schoolbestuur om te zien of er breder moet worden gecommuniceerd.

5. Evaluatie & rapportage

Voer direct na het incident een eerste evaluatie uit

Breng de eerste technische en praktische evaluatiepunten in kaart. Wat ging er goed, wat kan er beter en wat ontbrak er? Wat is er nodig voor een effectieve en vlotte reactie op de crisis.

Identificeer stappen om besmettingen in de toekomst te voorkomen

Welke maatregelen waren nog niet getroffen waardoor besmetting mogelijk was? Wat kun je doen om toekomstige kwaadwillenden buiten de deur te houden? Denk hierbij aan kwetsbare systemen uitfaseren, updates sneller uitvoeren of een besmetting eerder detecteren. Ook andere basismaatregelen kunnen bijdragen, bijvoorbeeld het invoeren van multifactor-authenticatie.

Bijlage: Verdieping

Sommige stappen uit het stappenplan zijn complex, daarom worden hieronder een aantal onderdelen verder toegelicht.

Toelichting bij stap 2: Schade beperken

Stop verdere verspreiding

Koppel direct systemen los van het netwerk (op alle interfaces: bekabeld, wifi of mobiel) waarvan is vastgesteld of het vermoeden bestaat dat ze gecompromitteerd zijn (met ransomware). Loskoppelen kan door de bekabeling los te halen, de wifi uit te schakelen of door de vliegtuigmodus te activeren. Wanneer virtuele machines gebruikt worden, schakel deze dan uit in het managementdashboard. Ontkoppel ook externe media van de apparaten zoals USB-opslag, mobiele telefoons of andere externe apparaten.

Zet systemen niet uit, maar breng ze in slaapstand of mogelijk sluimerstand (indien beschikbaar, bijvoorbeeld op laptops). Dit om de toestand van het systeem niet te verstoren, het verlies van eventueel aanwezig sleutelmateriaal te voorkomen en om geen forensische sporen te verliezen voor mogelijk onderzoek.

Blokkeer of deactiveer alle accounts die (mogelijk) bij de ransomwareaanval betrokken zijn. Reset wachtwoorden voor administrator- en andere systeem- of servicesaccounts.

Overweeg bij een grote aanval om netwerkinfrastructuur, zoals wifi, routers en switches en internetconnectiviteit te ontkoppelen om de verspreiding te stoppen en de hackers de toegang tot het netwerk te blokkeren. Verbreek de verbinding met netwerken of netwerkdelen die nog niet zijn getroffen door de ransomware.

Back-up verbindingen moeten worden verbroken en lopende back-up processen moeten worden stopgezet. Stel bestaande back-ups veilig door ze offline te halen.

Als er al kwaadaardige ip-adressen bekend zijn, laat deze dan direct blokkeren door de ICT-beheerder of ICT-leverancier.

Stel bewijsmateriaal veilig

Het verzamelen van bewijslast is cruciaal voor verder onderzoek naar de ransomwarebesmetting. Onderneem de volgende stappen om de bewijslast te verzamelen:

- Stel loggingdata veilig, zoals die van het netwerk, de firewalls, applicaties en van de endpointbescherming.
- Stel servers veilig die nodig zijn voor verder onderzoek en overweeg hier een volledige kopie van te maken.
- Stel verdachte e-mails veilig die gebruikt zijn om malware binnen het netwerk te brengen of waarmee gegevens gestolen zijn.
- Leg vast welke accounts zijn misbruikt of aangemaakt voor kwaadaardige acties.

Toelichting bij stap 3: Onderzoek

Start een onderzoek naar de ransomware

Bepaal om welke ransomware het gaat

In sommige gevallen bevat het losgeldverzoek een duidelijke verwijzing naar een ransomwaregroep of een specifieke soort ransomware. Als het minder duidelijk is welke partij er achter de aanval zit, kan onderzoek worden gedaan naar de indicatoren van de aanval. Denk hierbij aan de ip-adressen waarmee aanvallen zijn uitgevoerd, communicatiekanalen waarmee met de aanvallers is onderhandeld en Bitcoin-adressen.

Hoe zijn de aanvallers binnengekomen?

Het is belangrijk om 'Patient Zero' te identificeren om te begrijpen hoe de aanvaller binnengekomen is. Probeer te achterhalen welke gebruiker of systeem als eerste getroffen is door de ransomware. Je kunt onder meer nagaan waar ongebruikelijke activiteiten als eerste ontstonden. Er kan onder meer worden gezocht naar ongebruikelijke activiteit zoals:

- Die ontstaan zijn na ontvangst van een phishing mail.
- Communicatie met Command and Control(C2) servers.
- Installatie van veelvoorkomende ransomware-gerelateerde tooling zoals een keylogger, exploitatie van een kwetsbaarheid middels Metasploit, uitvoering van Mimikatz of Cobalt Strike.

Zijn er gegevens gestolen?

Gegevens kunnen op meerdere manieren gestolen worden, bijvoorbeeld via e-mails met bijlagen die aanvallers naar gecompromitteerde mailadressen sturen. Zoek in het netwerk of er gegevens naar opslagdiensten zijn verzonden zoals OneDrive, Dropbox, en WeTransfer. Laat je netwerkbeheerder zoeken naar ongebruikelijke netwerkgedragingen, zoals afwijking in hoeveelheid verkeer naar het internet, verdachte ip-adressen of ongebruikelijke tijdstippen.

Hebben de aanvallers nog toegang tot het schoolnetwerk?

Hou het netwerkverkeer in de gaten om ongebruikelijke netwerkgedragingen te detecteren. Zijn er ongebruikelijke inlogpogingen op ongebruikelijke tijden en wordt er verbinding gemaakt met verdachte ip-adressen? Blokkeer deze activiteit en registreer de kwaadaardige activiteiten om te gebruiken als bewijs.

Indien mogelijk: Monitor de eindgebruikerssystemen op verdachte processen en gedragingen met de End-Point Detection and Response (EDR) oplossing van jouw school.

Toelichting bij stap 4: Herstel

Stel een herstelplan op voor je systemen en activiteiten

Overweeg bij een grote aanval het netwerk en bijhorende systemen parallel aan de bestaande omgeving op te bouwen. Importeer geen systemen of gegevens zonder deze grondig te controleren op de aanwezigheid van malware. Sluit geen systemen op de schone omgeving aan die verbonden zijn geweest met de besmette omgeving.

Bij een grote aanval met mogelijke compromittatie van de Active Directory is het soms niet mogelijk om parallel aan de bestaande omgeving een nieuwe omgeving op te bouwen. Overweeg dan om een nieuwe rechtenstructuur op te bouwen met nieuwe accounts, waaronder ook beheer- en serviceaccounts, en alle oude accounts (permanent) te verwijderen.

Scan back-ups op malware voordat deze worden hersteld. De kwaadwillenden zijn mogelijk al langere tijd aanwezig in het netwerk, waardoor malafide bestanden in de back-ups terecht kunnen zijn gekomen. Herstel de systemen van de getroffen gebruikers middels back-ups. Valideer dat deze back-ups niet gecompromitteerd zijn. Herstel alleen van back-ups wanneer je er zeker van bent dat deze niet meer geïnfecteerd zijn.

Verhelp de bekende kwetsbaarheden in de systemen en software. Installeer updates en patches waar nodig.

Deel (technische) informatie over het incident met de politie. Dat kan bij een aangifte, maar ook los van een aangifte. Dit kan de (internationale) opsporing en verstoring van dadergroepen helpen en het kan leiden tot het notificeren van andere (potentiële) slachtoffers.

Test en verifieer of het afwijkende gedrag (o.a. netwerkverkeer) is verdwenen na het herstellen van alle systemen en processen. Monitor het netwerk enige tijd extra intensief om er zeker van te zijn dat de aanvaller uit het netwerk verdwenen is en er niet meer in terug kan komen.

Toelichting bij Stap 5: Evaluatie en rapportage

Gebruik de documentatie die tijdens crisis is gemaakt, zoals het logboek en de crisisagenda, om de tijdlijn van de crisis na te gaan. Stel vast wat er precies is gebeurd gedurende de gehele crisis. Waren er procedures omtrent bedrijfscontinuïteit of incidentresponse aanwezig en waren deze bruikbaar? Was er informatie die je eerder had willen hebben om sneller beslissingen te nemen of om mitigerende acties te ondernemen? Was de informatiedeling met de stakeholders adequaat, of zou het beter kunnen? Stel met deze resultaten preventieve en reactieve maatregelen op om het crisisproces te verbeteren.

Bepaal ook welke maatregelen nodig zijn om de technische oplossingen te verbeteren. Stel daartoe vast hoe het mogelijk was dat de ransomware het netwerk binnenkwam. Stel maatregelen op om deze kwetsbaarheden te verhelpen. Stel vast welke middelen en tools nodig zijn om soortgelijke aanvallen te detecteren, analyseren en mitigeren. Stel vast welke indicatoren (IOCs) van deze aanval gebruikt moeten worden om de configuraties van de eigen systemen te versterken.

Verder lezen na de crisis

- Business Continuity Management – Aanpak IBP
- Incident Management - Aanpak IBP
- 11 Basismaatregelen – Aanpak IBP
- Back-up en herstelplan – Aanpak IBP

Bijlage: Logboek

Incidentgegevens

Incident-ID: [Unieke identificatie voor dit incident]

Datum en tijd van detectie: [Tijdsstip waarop het incident voor het eerst werd gedetecteerd]

Beschrijving van het incident: [Korte samenvatting van het incident]

Incidentresponsteam (IRT) Informatie

Naam	Rol	Telefoonnummer	E-mail
	Voorzitter		
	Secretaris		
	Cybersecurity expert		
	Privacy expert		
	Communicatie		

Incident tijdslijn

Tijdstempel	Activiteit/beslissing	Verantwoordelijke	Opmerkingen
	Incident gedetecteerd	[Naam/Rol]	Korte beschrijving van de detectie
	Initiële beoordeling	[Naam/Rol]	Voorlopige analyse van het incident
	Beperkende maatregelen	[Naam/Rol]	Acties om de impact te beperken
	Communicatie	[Naam/Rol]	Meldingen aan belanghebbenden
	Onderzoek	[Naam/Rol]	Gedetailleerde inspectie van het incident
	Bewijsverzameling	[Naam/Rol]	Verzamelen van relevante logs en gegevens
	Beslissing over escalatie	[Naam/Rol]	Bepalen of verdere escalatie nodig is
	Herstelmaatregelen	[Naam/Rol]	Stappen om de normale werking te herstellen
	Leerpunten	[Naam/Rol]	Evaluatie na het incident en aanbevelingen

Bijlage: Agenda crisisoverleg

Datum:	
Locatie:	
Aanwezig:	
Afwezig:	

1. **Opening**

Doel/status bijeenkomst, vergaderfrequentie, rol van de aanwezigen, juiste inhoudelijk deskundigen, lopende zaken stilleggen, vervanging, afspraken vergaderdiscipline, actiepunten, eindproducten en voortgang.

2. **Beeld**

Matrix van feiten, onzekerheden, maatregelen, percepties van bijvoorbeeld publiek en medewerkers, (sociale) media.

3. **Oordeel**

Welke kant kan deze calamiteit/crisis opgaan? Wat is realistisch, wat is het worstcasescenario, wat voor scenario verwachten we?

4. **Besluit**

Welke maatregelen kunnen worden genomen, bij voorkeur op basis van advies inhoudelijk deskundige?

5. **Communicatie**

Welke strategie, wat moet de boodschap zijn, zowel in- als extern?

6. **Actiepunten vaststellen**

Prioriteiten en volgende vergadering.

School CERT Laatst geupdate 02-10-2024

Voor ondersteuning: support@kennisnet.nl / 0800 321 22 33

Voor vragen over het School-CERT: cert@kennisnet.nl