Rapportage ransomware

Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar

Rapportage oktober 2024

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Samenvatting

Organisaties onvoldoende weerbaar tegen ransomware door gebrekkige beveiliging

In 2023 zijn er 178 unieke ransomware-aanvallen gemeld aan de Autoriteit Persoonsgegevens (AP). Uit onderzoek van de AP blijkt dat bij twee op de drie getroffen organisaties de basisbeveiliging niet op orde was. Daarom roept de AP organisaties op om de basisbeveiliging op orde te brengen om zo weerbaar te zijn tegen ransomware.

Basisbeveiliging op orde
De AP roept organisaties op om in ieder geval:
1. te zorgen voor meerfactorauthenticatie (MFA).
   En het gebruik ervan af te dwingen onder medewerkers;
2. een goed wachtwoordbeleid op te stellen;
3. updates op tijd uit te voeren. Zeker bij bekende kwetsbaarheden
   (zoals 'Common Vulnerabilities and Exposures' of CVE's);
4. te zorgen voor voldoende netwerksegmentatie.

Nieuwe trend: privacy slachtoffers extra geschaad door dubbele afpersing

In ongeveer 50% van de onderzochte ransomware-aanvallen versleutelden cybercriminelen niet alleen systemen, maar stalen ze ook (persoons)gegevens. Dit is extra schadelijk voor de privacy van de mensen van wie de gegevens zijn, omdat hun gegevens op het dark web terecht kunnen komen. Bovendien neemt hiermee de kans op identiteitsfraude, phishing en oplichting toe.

Niet betalen is de norm

Uit het onderzoek van de AP blijkt dat ongeveer 9% van de onderzochte organisaties besluit om losgeld te betalen na een ransomware-aanval. Het betalen van losgeld is echter geen oplossing of beveiligingsmaatregel. Het geeft namelijk geen zekerheid dat gelekte persoonsgegevens niet alsnog worden doorverkocht of gepubliceerd. Bovendien houdt het criminaliteit in stand. Daarom is niet betalen de norm.

Het onderzoek

Bij veel ransomware-aanvallen zijn persoonsgegevens betrokken. Dit kan grote risico's opleveren voor de slachtoffers. Zij kunnen phishingberichten ontvangen of slachtoffer worden van identiteitsfraude. Vanwege de grote risico's moeten organisaties dit soort datalekken vrijwel altijd melden aan de AP en aan de slachtoffers. Door deze meldplicht heeft de AP een breed beeld van de aard en omvang van ransomware-aanvallen in Nederland.

Meer inzicht in ransomware-aanvallen helpt de Nederlandse samenleving er weerbaarder tegen te zijn, wat de bescherming van persoonsgegevens ten goede komt. Voor dit onderzoek heeft de AP incidentrapporten, datalekmeldingen, e-mailuitwisselingen, datalekregisters en technische details geanalyseerd van 90 ransomware-aanvallen.

2. Basismaatregelen zijn niet op orde

Twee op de drie door ransomware getroffen organisaties hadden de basisbeveiliging niet op orde. Hierdoor waren ze onvoldoende weerbaar tegen een ransomware-aanval. De AP maakt zich ernstig zorgen over het beveiligingsniveau van de onderzochte organisaties. De vier belangrijkste missende aspecten van basisbeveiliging zijn:

1. Implementeren van meerfactorauthenticatie (MFA);
2. sterk wachtwoordbeleid;
3. adequaat reageren op algemeen bekende kwetsbaarheden (ook wel 'Common Vulnerabilities and Exposures' of CVE's genoemd);
4. voldoende segmentatie van het netwerk.

Dit hoofdstuk gaat over 63 van de 90 onderzochte aanvallen. Bij de overige 27 incidenten was het namelijk niet duidelijk van welke kwetsbaarheden de cybercriminelen gebruik hebben gemaakt om binnen te komen.

2.1 Meerfactorauthenticatie (MFA) ontbreekt

In 52% van de onderzochte gevallen werd expliciet genoemd dat MFA niet aanstond of afgedwongen werd bij de getroffen organisatie. Dit betekent niet dat MFA in de andere 48% wel op orde was; daar werd alleen niet expliciet genoemd dat MFA ontbrak. Het aantal geslaagde aanvallen waarbij MFA niet aanstond, ligt waarschijnlijk hoger dan de 52% die uit dit onderzoek naar voren komt.

De AP vindt het zorgelijk dat MFA nog steeds geen standaard onderdeel is van het cybersecuritybeleid van sommige Nederlandse organisaties. De AP besteedde in de rapportage datalekken 2020 al aandacht aan hoe MFA de impact van een datalek kan verkleinen of zelfs voorkomen.[1]

Wat is MFA?

MFA betekent dat er altijd twee of meer 'factoren' zijn om mee in te loggen: iets dat je weet (bijvoorbeeld een wachtwoord), iets dat je hebt (bijvoorbeeld een tijdelijke code via een app) of iets dat onderdeel is van jou (bijvoorbeeld een vingerafdruk)[2]. Deze maatregel is relatief goedkoop en gemakkelijk te implementeren. Organisaties gebruiken MFA dan ook steeds vaker. Inloggen met een extra stap levert gebruikers veel extra bescherming op.

2.2 Slecht wachtwoordbeleid

De tweede basismaatregel die organisaties nog steeds onvoldoende op orde hebben, is het implementeren van een goed wachtwoordbeleid. Ook dit is zorgelijk, aangezien de AP er in een richtsnoer van 2021 al uitgebreid aandacht aan besteedde.[3]

Hoe streng een wachtwoordbeleid moet zijn, verschilt per organisatie. Wel zijn er minimale eisen waaraan iedere organisatie zou moeten voldoen. Hieraan voldeden 15 van de 63 onderzochte organisaties niet. Slecht wachtwoordbeleid werd hier expliciet genoemd als reden voor het slagen van de ransomware-aanval of voor de impact van de aanval. Zo werd bijvoorbeeld hetzelfde wachtwoord gebruikt voor alle adminaccounts. Ook de mensen die de systemen gebruiken, moeten zorgen voor een sterk wachtwoord. De AP heeft al eerder tips gegeven over sterke wachtwoorden.[4] In combinatie met MFA kunnen sterke wachtwoorden een behoorlijk deel van de ransomware-aanvallen voorkomen.

2.3 Updates niet op tijd uitvoeren

De derde basismaatregel die bij de onderzochte organisaties ontbrak, was het op tijd uitvoeren van updates. Specifiek als het ging om een updates die een 'Common Vulnerability and Exposure' (CVE) tegengaan.

Voeren organisaties na het bekend worden van een CVE niet snel genoeg updates uit, dan zijn ze extra kwetsbaar voor ransomware-aanvallen. Bij 8 van de 63 onderzochte organisaties bleek dat het geval. In 6 van deze 8 gevallen waren de oplossingen voor de kwetsbaarheden, de 'patches', ook al langer dan een maand bekend. In het onderzoek kwamen zelfs meerdere kwetsbaarheden naar voren van meer dan een jaar oud. De software, en daarmee de organisatie, was dus al meer dan een jaar kwetsbaar, terwijl de update wel beschikbaar was.

Wat zijn Common Vulnerabilities and Exposures (CVE's)?

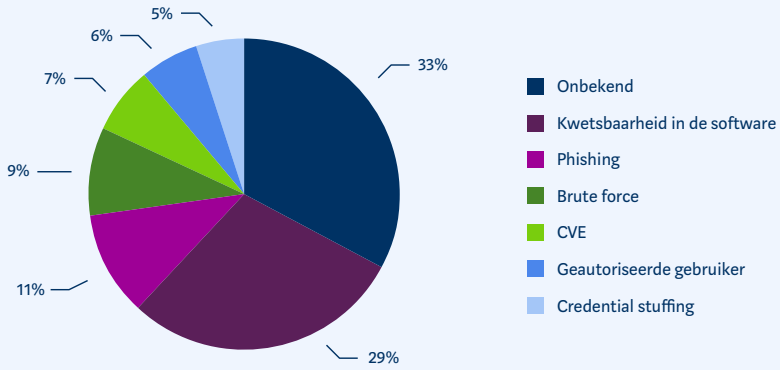
Bij CVE's deelt een softwareleverancier, overheidsorganisatie of onafhankelijk onderzoeker een kwetsbaarheid online om organisaties ervoor te waarschuwen. Zo kunnen organisaties waar mogelijk de kwetsbaarheid mitigeren, bijvoorbeeld door te updaten. Door het online delen hebben cybercriminelen ook toegang tot deze informatie. Zij kunnen de informatie gebruiken voor een ransomware-aanval. Snel handelen is voor organisaties dus essentieel.

Eerste toegangspunt tot de systemen ('initial access')
Zoals te zien in figuur 1, waren er meerdere manieren waarop cybercriminelen toegang kregen tot de systemen van de onderzochte organisaties. Dit eerste toegangspunt tot systemen wordt ook wel 'initial access' genoemd.

Een veelgebruikte manier om binnen te komen is via een kwetsbaarheid in de software. In sommige gevallen kon vastgesteld worden dat dit kwam door een CVE. In dit onderzoek waren CVE's kwetsbaarheden die langer dan een maand bekend waren en niet werden opgelost.

Een aantal keer kregen cybercriminelen toegang via een bestaand account bij de organisatie. Dit kan bijvoorbeeld door middel van 'credential stuffing', waarbij eerder gelekte inloggegevens gebruikt worden. En bij 'brute force' proberen cybercriminelen met behulp van computerprogramma's (willekeurige) inloggegevens om toegang te krijgen tot de systemen. Als geen van deze technieken vastgesteld kon worden, maar er wel ingelogd was met bekende gegevens, dan valt dit in de figuur onder de categorie 'geautoriseerde gebruiker'.

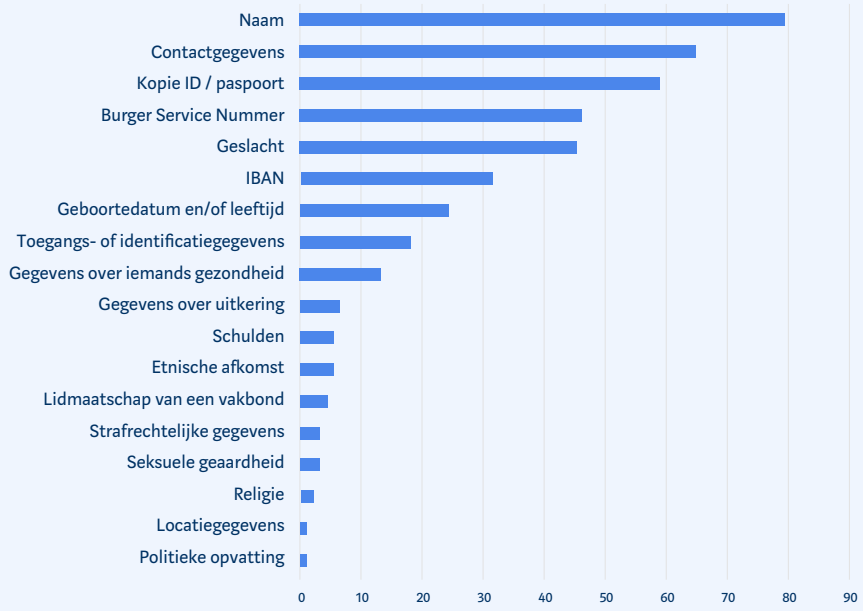
FIGUUR 1



Welke persoonsgegevens?

Figuur 2 laat zien welke soorten persoonsgegevens hoe vaak lekten bij een ransomware-aanval. Het valt op dat naam, adres, telefoonnummer en e-mailadres bij bijna iedere aanval worden gelekt. Daarnaast is het zeer zorgelijk dat in 75% van de gevallen kopieën van ID-bewijzen en paspoorten in verkeerde handen kwamen, met een hoger risico op identiteitsfraude tot gevolg.

FIGUUR 2



Figuur 2 heeft betrekking op 79 van de 90 organisaties. Bij de overige elf organisaties varieerde het sterk welke soorten persoonsgegevens lekten.

2.4 Weinig tot geen netwerksegmentatie

De vierde en laatste basismaatregel die niet op orde was bij de onderzochte organisaties, is het gebrek aan (voldoende) netwerksegmentatie. Hiervan was sprake bij 12 van de 63 ransomware-aanvallen.

Netwerksegmentatie is een beveiligingsmaatregel die vertragend werkt. Hoe langer de cybercriminelen bezig zijn in het netwerk en 'vreemde' acties uitvoeren, hoe groter de kans dat de beveiligingssoftware of een systeembeheerder dit opmerkt en de aanval (gedeeltelijk) kan voorkomen. Bij meerdere organisaties bleek netwerksegmentatie de reden dat de cybercriminelen maar een gedeelte van het netwerk konden versleutelen. Bovendien vergroot netwerksegmentatie de kans dat er back-ups beschikbaar blijven, waardoor een organisatie snel weer aan het werk kan. Dit voorkomt bovendien dat de organisatie de moeilijke afweging moet maken om wel of niet te betalen om weer toegang te krijgen tot systemen.

Wat is netwerksegmentatie?

Netwerksegmentatie houdt in dat niet alles van een netwerk op dezelfde plek staat. Data staan verspreid over verschillende servers die fysiek of met een digitale beveiligingslaag (bijvoorbeeld een firewall) van elkaar gescheiden zijn. Deze spreiding maakt het veel lastiger voor cybercriminelen om in het systeem toegang te krijgen tot bepaalde 'rechten' waarmee ze het volledige netwerk zouden kunnen versleutelen. Hoe lastiger dit is en hoe meer tijd dit kost, hoe groter de pakkans en hoe kleiner de buit.

3. Nieuwe trend: dubbele afpersing

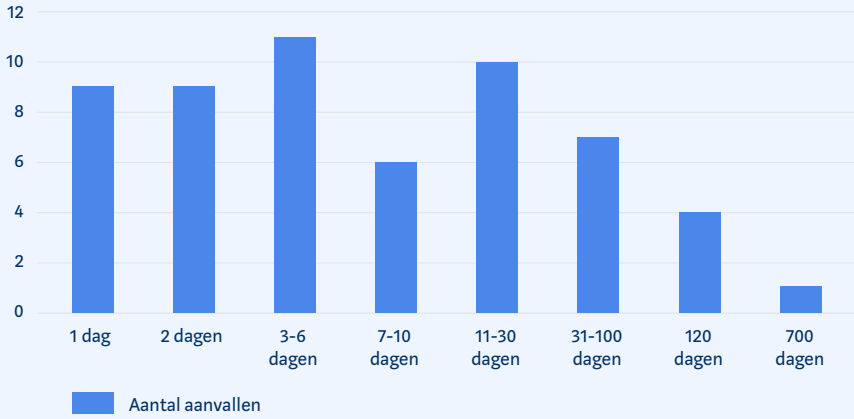
In Nederland is een nieuwe trend te zien: dubbele afpersing. In ongeveer de helft van de onderzochte aanvallen (44 van de 90) werd de organisatie niet alleen getroffen door ransomware – waarna losgeld werd geëist – maar stalen de cybercriminelen ook gegevens. Daarnaast hadden zeker nog 8 organisaties hiervan een vermoeden. De cybercriminelen dreigden met publicatie of verkoop van de gestolen (persoons)gegevens als de organisatie niet betaalde.

De gegevens die de cybercriminelen buitmaken, zijn vaak persoonsgegevens. Dubbele afpersing levert daardoor een dubbel risico op voor de mensen van wie de gegevens zijn. Niet alleen stelen de cybercriminelen gegevens; zij publiceren of verkopen de gegevens daarna ook nog eens op het dark web. Het gevaar is bijzonder groot als gestolen gegevens met elkaar gecombineerd worden. Waar een enkel gegeven soms weinig zegt, kan een combinatie van gegevens een gedetailleerd profiel van iemand opleveren. Criminelen gebruiken zulke profielen voor gerichte phishingmails of identiteitsfraude. In 2023 deden ruim 7000 mensen melding van identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude (CMI)[5].

Hoe lang waren ze binnen?

Figuur 3 laat zien hoe lang de cybercriminelen binnen waren op het netwerk van de getroffen organisatie. Het gaat om het eerste moment dat de cybercriminelen duidelijk actief waren op het netwerk, tot het moment dat de cybercriminelen het netwerk versleutelden. In sommige gevallen zat hier veel tijd tussen, zonder dat de cybercriminelen in de tussentijd actief waren. Bij de uitschieters aan de rechterkant van de grafiek zijn de cybercriminelen bijvoorbeeld niet twee jaar lang constant bezig geweest, maar hebben ze na de initiële toegang een periode niet omgekeken naar de organisatie. Pas op een (veel) later moment zijn ze overgegaan op versleuteling. In die gevallen hadden organisaties dus veel tijd om de hack op te merken en verdere schade te voorkomen.

FIGUUR 3

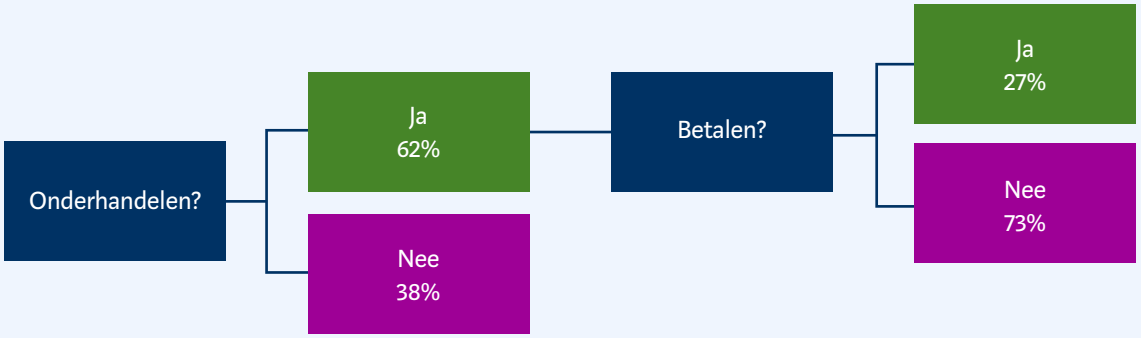


4. Niet betalen is de norm

Van de 90 onderzochte organisaties betaalden er minimaal 8 losgeld aan de cybercriminelen (figuur 4). De AP vindt het een goede zaak dat verreweg de meeste organisaties geen losgeld betalen. Betalen houdt namelijk een illegaal systeem in stand. Hoe minder vaak organisaties besluiten te betalen na een ransomware-aanval, hoe minder aantrekkelijk Nederland wordt voor cybercriminelen. Dat komt de bescherming van persoonsgegevens van Nederlanders ten goede.

Bovendien is betalen geen garantie dat de cybercriminelen zich aan hun woord houden. In dit onderzoek heeft de AP gezien dat een organisatie na betaling géén toegang terugkreeg tot de systemen, ondanks de belofte van de cybercriminelen. De systemen bleven versleuteld en de gestolen (persoons)gegevens belandden alsnog op het dark web. Van de cybercriminelen ontbrak ieder spoor.

FIGUUR 4



Onderhandelen en betalen?
Figuur 4 laat zien wat organisaties doen nadat ze een ransomware-aanval ontdekken. Organisaties hebben de keuze om contact op te nemen met de cybercriminelen of niet, en om te betalen of niet. Het grootste gedeelte van de organisaties neemt contact op om erachter te komen wat de cybercriminelen hebben buitgemaakt. Na dat eerste contact, vaak via een privéverbinding op het dark web, besluiten de meeste organisaties niet te betalen. Van de 62% die besluit te onderhandelen, betaalt uiteindelijk 27%.

5. Bronnen

1. Jaarrapportage meldplicht datalekken 2020 | Autoriteit Persoonsgegevens
2. Techblogpost: factoren in authenticatie | Autoriteit Persoonsgegevens
3. Guidelines EDPB over voorbeelden melding van inbreuken in verband met persoonsgegevens
4. Techblogpost: sterke wachtwoorden in de praktijk | Autoriteit Persoonsgegevens
5. Cijfers: Centraal Meldpunt Identiteitsfraude | RvIG

AUTORITEIT
PERSOONSGEGEVENS