Jaarbeeld Ransomware 2024

Project Melissa
Publiek-private samenwerking op ransomware

Samen brengen wij ransomware in Nederland in beeld

In 2024 hebben het Nationaal Cyber Security Centrum (NCSC), de Politie, het Openbaar Ministerie, Cyberveilig Nederland en cybersecuritybedrijven maandelijks informatie over ransomware-incidenten uitgewisseld in het kader van project Melissa (zie 'meer informatie'). Deze uitwisseling geeft beter inzicht in hoe vaak en op welke manier organisaties in Nederland worden getroffen door ransomware incidenten. Want over hoe meer actuele informatie we beschikken, hoe effectiever we ransomware kunnen bestrijden.

In dit jaarbeeld baseren we ons op gecompileerde maandelijkse incidentinformatie van Computest, DataExpert, Deloitte, Eye Security, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, het NCSC en de aangifte cijfers van de Politie over de periode van januari t/m december 2024.

National Cyber Security Centre Ministry of Security and Justice · OM · POLITIE · CYBERVEILIG NEDERLAND

Één jaar aan gedeelde ransomware-incidenten in beeld

Naar schatting **121** unieke incidenten

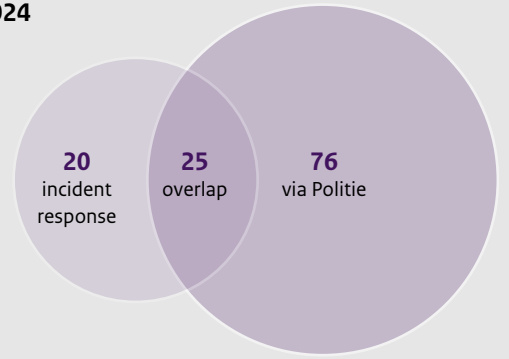
Via maandelijkse terugkerende uitvraag en aangiftes van januari t/m december 2024

Via **9** cybersecurity-dienstverleners, NCSC en de Politie

Samen meer zicht op ransomware

Door incident-response-data met aangiftedata te combineren maken we incidenten inzichtelijk: 45 incidenten vanuit incident response en 101 incidenten vanuit de Politie met een overlap van 25 incidenten.

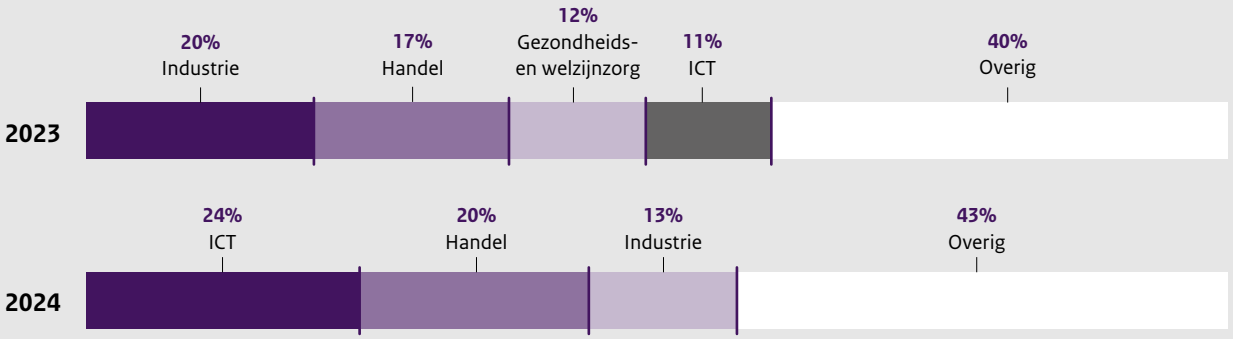
2024



Stijgende bereidheid tot betalen in NL

De bereidheid tot betaling van losgeld is met **11%** gestegen ten opzichte van vorig jaar. Deze procentuele stijging is te wijten aan een kleiner aantal slachtoffers in 2024 ten opzichte van 2023. In absolute cijfers gaat het om **10** slachtoffers (2023) en **13** slachtoffers (2024).

Top 3 getroffen sectoren ter vergelijking met vorig jaar



De top 3 getroffen sectoren is anders dan in 2023; ICT is de nieuwkomer met 24%.

Ransomware-incidenten volgen de gebaande paden voor toegang

2024

38%
Account take-over

33%
Misbruik van kwetsbaarheden

Net als vorig jaar wordt toegang meestal verkregen door misbruik van kwetsbaarheden en account-takeover. Zorg ervoor dat uw basismaatregelen op orde zijn.[1]

Veranderingen in het ransomware-landschap

Ransomwaregroepen komen en gaan, soms vanwege succesvolle Politie-acties, soms omdat ze in een andere samenstelling verder gaan. Begin 2024 **verdween BlackCat/ALPHV**. De voormalige affiliates stapten over naar andere groepen zoals **RansomHub**, die afgelopen jaar ook in Nederland actief is geweest.

Ook **Cactus** was dit jaar verantwoordelijk voor een aanzienlijke hoeveelheid slachtoffers in Nederland. Uit een gezamenlijke analyse binnen project Melissa bleek dat Cactus voor initial access misbruik had gemaakt van een kwetsbaarheid in Qlik Sense. Het scannen op kwetsbare servers en het informeren van potentiële slachtoffers hielp de mogelijke impact in Nederland te verminderen.

Nieuwe deelnemers welkom

Alleen samen maken we ons beeld van ransomware in Nederland completer en maken we een vuist tegen ransomware. Staat uw bedrijf ransomware slachtoffers bij? Dan bespreken wij graag met u de mogelijkheden en het belang van bijdrage aan deze statistieken. Mail voor meer informatie naar info@ncsc.nl.

Verantwoording cijfers

Dit jaarbeeld is gebaseerd op gegevens van cybersecurity-dienstverleners en de Politie. De incidenten zijn zorgvuldig beoordeeld door security-experts, die een scherpe afbakening van de definitie van ransomware hanteren.[2] Uit onderzoek blijkt dat grote en middelgrote organisaties (vanaf ca. 50 fte) in ongeveer 40% van de gevallen zichtbaar zijn in deze bronnen, terwijl dit voor het MKB slechts 10-15% is.[3] Dit suggereert dat het werkelijke aantal ransomware-aanvallen 2-3 keer hoger ligt voor grote en middelgrote bedrijven en tot 10 keer hoger voor kleine bedrijven. De hier genoemde cijfers bieden een schatting van unieke incidenten, aangezien volledige controle op dubbeltellingen door anonimisatie niet mogelijk is.

Meer informatie

Berg, B. van den, Weggemans, D., en Nobbenhuis, M. (2024). “Samenwerken tegen Ransomware: Evaluatie Melissa”, Samenwerken tegen Ransomware.

Eindnoten

1 Nationaal Cyber Security Centrum, “5 basisprincipes van digitale weerbaarheid”, 27 september 2024. https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes

2 “De naam ransomware is een samenvoeging van de woorden ransom (losgeld) en software. De aanvallers gijzelen data van het slachtoffer en gebruiken drukmiddelen om het slachtoffer over te halen te betalen.” Cyberveilig Nederland, “Cyberveilig Nederland publiceert Whitepaper Ransomware met leden, Politie en NCSC”. CVNL_Ransomware_def.pdf, pag. 4.

3 Meurs, T., Junger, M., Cruyff, M., & Van Der Heijden, P. G. (2024). Estimating the Number of Ransomware Attacks. Available at SSRN 4942706.