Jaarbeeld Ransomware 2023

Samen brengen wij ransomware in Nederland in beeld

In 2023 hebben het NCSC, de Politie, het Openbaar Ministerie en bij Cyberveilig Nederland aangesloten cybersecuritybedrijven maandelijks informatie over ransomware-incidenten uitgewisseld. Het doel van deze uitwisseling is om beter inzicht te krijgen 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 ransomware 2023 kijken we naar organisaties groter dan 100 fte en baseren we ons op incidentinformatie van Computest, DataExpert, Deloitte, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, het NCSC en de aangifte cijfers van de Politie.

Vragen of interesse?

Neem contact op via info@ncsc.nl

Project Melissa - Publiek Private Samenwerking Ransomware

National Cyber Security Centre
Ministry of Security and Justice

OM POLITIE CYBERVEILIG NEDERLAND

Één jaar aan cijfers via maandelijkse uitvragen over ransomware-incidenten in Nederland verkregen via incident-response-partijen, het NCSC en de Politie.

Één jaar aan gedeelde ransomware-incidenten in beeld

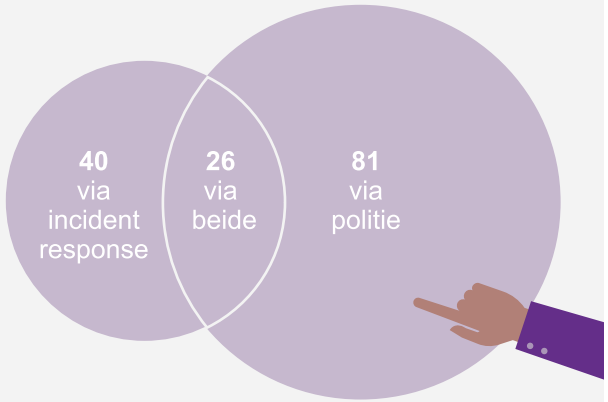
via anoniem delen naar schatting **147** unieke incidenten in zicht

via maandelijks terugkerende uitvraag van januari t/m december in 2023

via **8** cybersecurity-dienstverleners, het NCSC en de Politie zicht op organisaties door heel Nederland

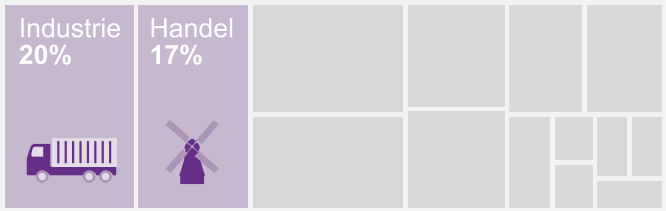
Samen meer zicht op ransomware

Door incident-response-data met aangiftedata te combineren zijn er meer incidenten in beeld.

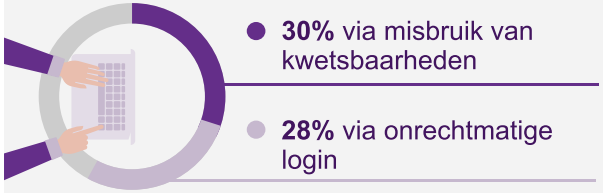


Industrie en handel vaak slachtoffer

Slachtoffers komen voor in alle sectoren, maar het meest in de industrie en handel (samen meer dan **1/3** van de jaarlijkse incidenten).



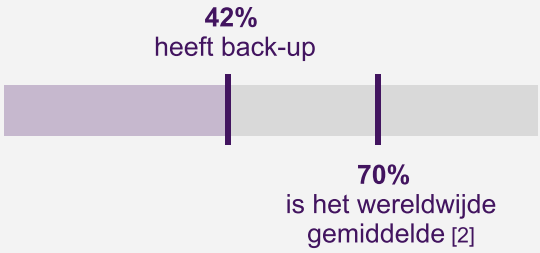
Ransomware-incidenten volgen de gebaande paden voor toegang



- **30%** via misbruik van kwetsbaarheden
- **28%** via onrechtmatige login

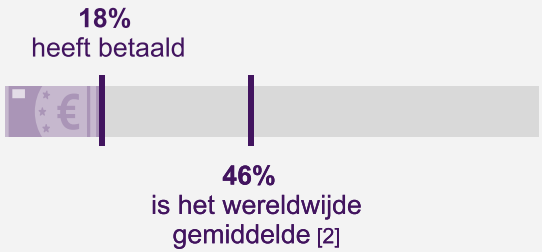
Ongeoorloofde toegang voorkomen? Zorg dan dat de basismaatregelen op orde zijn. [1]

Er zijn meer back-ups nodig



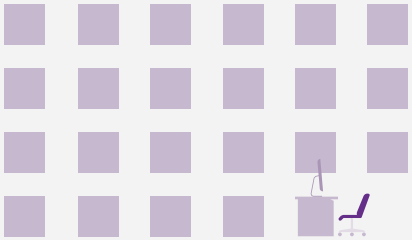
Jammer. Een goede back-up strategie is van groot belang om na een incident snel te herstellen. [3]

Betaalbereidheid binnen incidenten relatief laag



Positief! Want door niet te betalen geven we een sterk signaal tegen cybercriminelen. [4]

Dreiging vanuit groot aantal ransomware-families



Met **23** unieke ransomware-families is de dreiging opvallend breed. Informatiedeling en samenwerking is dus cruciaal.

Nieuwe deelnemers welkom

Alleen samen maken we ons beeld van ransomware in Nederland completer en maken we een vuist tegen ransomware. Staat uw bedrijf slachtoffers van ransomware bij? Dan bespreken wij graag met u de mogelijkheden en het belang van deelname aan project Melissa.

Verantwoording cijfers

Dit jaarbeeld compileert informatie over ransomware-incidenten bij grotere organisaties (vanaf ca. 100 fte), afkomstig van gespecialiseerde cybersecuritybedrijven. Incidenten zijn beoordeeld door security-experts die een scherpe afbakening van de definitie ransomware hanteren. Hierdoor kan dit jaarbeeld afwijken van andere jaarbeelden waarbij uitvraag is gedaan bij burgers en/of kleinere organisaties. Vanwege het anonimiseren van de data is perfect ontdubbelen niet mogelijk, vandaar dat we spreken over een schatting aan unieke incidenten.

Overige bronnen

[1] Nationaal Cyber Security Centrum, “Basismaatregelen cybersecurity”, Nationaal Cyber Security Centrum, 19 juli 2023. https://www.ncsc.nl/onderwerpen/basismaatregelen
[2] Sophos, “2023 Ransomware Report: Sophos State of ransomware”, SOPHOS. https://www.sophos.com/en-us/content/state-of-ransomware
[3] Nationaal Cyber Security Centrum, “Bescherm uw organisatie tegen het verlies van gegevens”, Nationaal Cyber Security Centrum, 6 juli 2023. https://www.ncsc.nl/onderwerpen/back-ups
[4] Meurs, T., Cartwright, E., Cartwright, A., Junger, M., Hoheisel, R., Tews, E., & Abhishta, A. (2023). Ransomware Economics: A Two-Step Approach To Model Ransom Paid. In Symposium on Electronic Crime Research, eCrime 2023 Advance online publication.