Jaarbeeld Ransomware 2023

Samen brengen wij ransomware in Nederland in beeld

Informatie over ransomware-incidenten wordt nog te weinig of te laat gedeeld. Hierdoor ontbreekt een actueel totaalbeeld en is ransomware-bestrijding minder effectief. Het NCSC, de Politie, het Openbaar Ministerie en Cyberveilig Nederland brengen hier verandering in en zijn het initiatief gestart om maandelijks informatie over actuele ransomware-incidenten te delen. Hiermee presenteren wij het eerste jaarbeeld ransomware gebaseerd op uitvragen van september 2022 t/m augustus 2023.

Dit jaarbeeld is gebaseerd op incident informatie van Computest, DataExpert, Deloitte, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, het NCSC en de aangifte cijfers van de Politie. De deelnemers delen hun informatie via SecureNed, een platform om veilig en geanonimiseerd vertrouwelijke informatie van publieke en private partijen te delen.

Project Melissa - Publiek Private Samenwerking Ransomware

National Cyber Security Centre
Ministry of Security and Justice

OM POLITIE CYBERVEILIG NEDERLAND

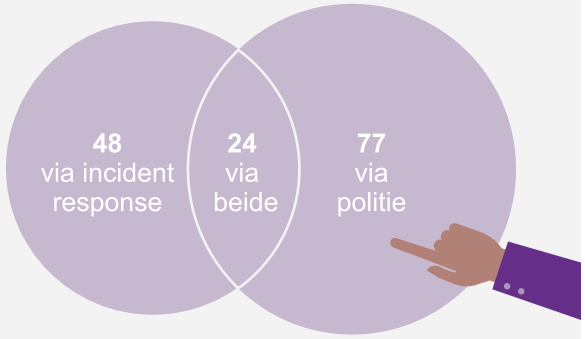
Één jaar aan cijfers via maandelijkse uitvragen over ransomware-incidenten in Nederland verkregen via incident-response-partijen, het NCSC en de Politie.

Één jaar aan ransomware-incidenten in beeld

- naar schatting **149** unieke incidenten
- **84** keer informatie gedeeld
- verdeeld over **12** maanden
- met **7** incident response partijen

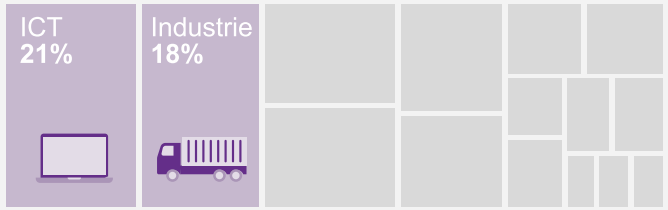
Samen meer zicht op ransomware

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

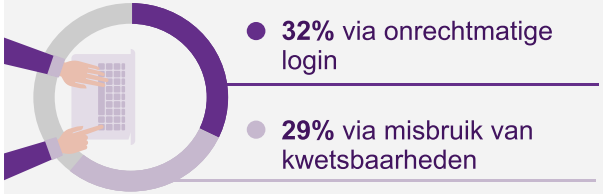


ICT en industrie vaak slachtoffer

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

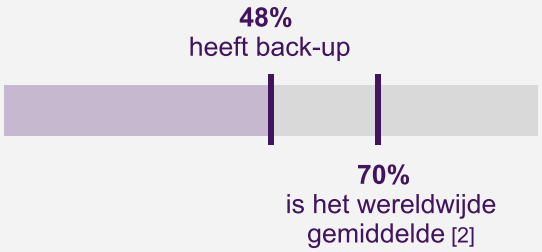


Ransomware-incidenten volgen de gebaande paden voor toegang



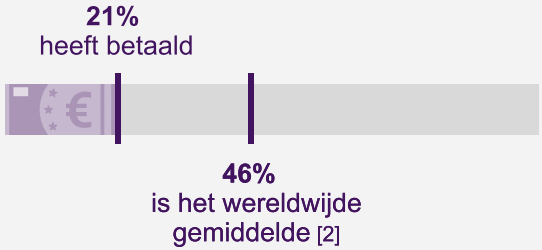
Ongeoorloofde toegang voorkomen? Zorg dus dat de basismaatregelen op orde zijn. [1]

Er zijn meer back-ups nodig



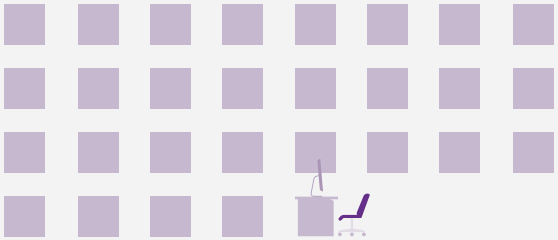
Jammer. Zorg voor goede back-up-strategie, zo kan je snel van incidenten herstellen. [3]

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 **29** 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 met incidentresponsactiviteiten? Dan bespreken wij graag met u de mogelijkheden en voordelen van deelnemen aan ons initiatief.

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.

Vragen of interesse?

Neem contact op via info@ncsc.nl

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.E., Tews, E., & Abhishta, A. (2023, under review). Ransomware Economics: A Two-Step Approach To Model Ransom Paid. Manuscript submitted for publication.