Onderzoeksrapport: Internet footprint MKB Brabant

Cyberweerbaarheid, ernstige gebreken worden bevestigd

Colofon

Datum
April 2023

Uitgave
ACA IT-Solutions
Beukenlaan 40-50
5651 CD Eindhoven
040-8800100
info@aca-it.nl

Auteurs
Geert Rademakers, Directeur
Michael Waterman, Cybersecurity Architect
Remco Wefels, Marketing & Communicatie
David Ruijs, Cybersecurity Consultant

Partners
MKB Eindhoven
Microsoft
Fortinet
Dell Technologies

Ondersteuning in de realisatie
Splend
Studenten Fontys ICT Hogeschool

Introductie

Ernstige gebreken zijn geconstateerd in de cyberweerbaarheid van het Brabantse MKB en dus is er werk aan de winkel voor het regionale bedrijfsleven. Dat is de algehele conclusie van het marktonderzoek-tweeluik van ACA IT-Solutions:

1. Cyberweerbaarheidsonderzoek MKB Brabant (fase 1, eind 2022)
2. Onderzoek internet footprint MKB Brabant (fase 2)

Fase 1: verbeterslagen dienen versneld te worden doorgevoerd

In fase 1 hebben bijna 200 Brabantse organisaties (2-999 FTE) een vragenlijst doorlopen, waarbij zij hun visie op cybersecurity gaven en de wijze waarop dit in hun organisatie is gerealiseerd. Dit onderzoek is eind december 2022 gepubliceerd. Toen werd geconcludeerd:

"Het MKB staat volop in de belangstelling van cybercriminelen. Een inhaalslag is hoog nodig. Kijkend naar de onderzoeksresultaten zijn er quick wins te behalen bij veel organisaties door een aantal basisprincipes. Dit staat ook in ons onderzoeksrapport vermeld en het advies is om, op brede schaal, versneld door te voeren. Hiermee kunnen al veel aanvallen gepareerd worden dan wel onschadelijk worden gemaakt. Dit dient gecombineerd te worden met een structurele verbeterslag en permanente aandacht op directieniveau."

Fase 2: hoe kijkt een cybercrimineel naar jouw organisatie?

Een geselecteerd aantal van 30 onderzochte bedrijven heeft vervolgens geparticipeerd in een verdiepingsslag: fase 2 van het onderzoek. Waar in de eerste fase de visie en perceptie van de ondervraagde centraal stond, hebben we in de tweede fase de 'bril opgezet van de cybercrimineel'. Zo zijn de openbare veiligheidsrisico's van de organisaties getoetst middels een zogeheten OSINT-scan.

OSINT staat voor Open Source Intelligence en is een onderzoeksmethodiek die cybercriminelen als basis gebruiken ter oriëntatie op een cyberaanval. Deze methodiek bestaat grotendeels uit automatische scans, waarmee cybercriminelen het web afstruinen naar zwakke plekken van bedrijven, die hierdoor vanzelf boven komen drijven. Regelmatig horen wij uit het bedrijfsleven: "Waarom zou een cybercrimineel ons bedrijf hier in Brabant willen aanvallen?" Een enorme misvatting, want een cybercrimineel geeft vaak niet om geografische gegevens. Doordat kwetsbaarheden van jouw bedrijf tijdens scans verschijnen, word je een doelwit.

We onderzochten of en hoe betreffende organisaties op het open, dark- en deepweb zichtbaar zijn voor kwaadwillenden en daardoor een verhoogd risico lopen om aangevallen te worden.

Ook dit verdiepende onderzoek wijst uit dat de cyberweerbaarheid van het MKB in Brabant nog veel te wensen overlaat. Het besef lijkt er nog onvoldoende binnen organisaties dat er meer gevraagd wordt om cybercriminelen buiten de deur te houden. Externe kwetsbaarheden en de mogelijkheden om daar misbruik van te maken zijn er legio. Dit is een vooronderzoek dat cybercriminelen in de praktijk uitvoeren. Ofwel: als wij dit kunnen vinden, dan kunnen zij dat ook.

Beukenlaan 40-50 | 5651 CD Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

Managementsamenvatting:

Er is in openbare bronnen veel informatie te vinden van MKB-bedrijven in de provincie Noord-Brabant. Dit kan voor cybercriminelen van grote waarde zijn bij het voorbereiden en actief uitvoeren van een cyberaanval. Dat is een zorgwekkende constatering. Een deel van de onderzochte organisaties zet zichzelf hiermee nadrukkelijk op de kaart bij kwaadwillenden.

Navolgend enkele conclusies naar aanleiding van de onderzoeksmethodieken die we op de onderzochte bedrijven loslieten:

1. Achterstallige updates en patches creëren kwetsbaarheden

Bedrijfsnetwerken bestaan tegenwoordig uit veel componenten. Daarin kunnen zwakheden ontstaan, die worden ontdekt door de fabrikant zelf of een externe partij zoals een cybersecurity specialist of een ethical hacker. Bij constatering wordt er internationale melding gemaakt en als CVE (Common Vulnerabilities and Exposures) in een database toegevoegd met daarin informatie hoe deze kwetsbaarheid te verhelpen, vaak door een patch of update door te voeren.

Dit wordt door de IT-/softwarefabrikant bekend gemaakt, waarna de werkzaamheden kunnen worden uitgevoerd door de IT-verantwoordelijke van jouw bedrijf. Tussen het moment van de bekendmaking en de update is jouw bedrijf kwetsbaar. Tijdens het marktonderzoek constateerden we dat bedrijven tal van updates niet hebben doorgevoerd, waarvan een significant aantal met hoge risico's.

Patchmanagement blijkt bij bedrijven onvoldoende op orde en het is zeer aannemelijk dat bedrijven niet goed in beeld hebben welke IT-middelen en systemen gebruikt worden en welke updates deze nodig hebben. Dat blijkt uit de oudheid van een groot aantal CVE's. Er wordt dus niet structureel patchmanagement uitgevoerd. Bovendien heeft 2/3 deel van de ontdekte CVE's al een publieke exploit. Dat betekent dat er code online beschikbaar is voor cybercriminelen, waarmee de kwetsbaarheid actief kan worden misbruikt.

2. E-maildomeinen zijn onvoldoende beveiligd volgens de huidige standaarden

Om e-maildomeinen te beschermen tegen ongeoorloofd gebruik (e-mail spoofing, CEO-fraude, phishing) kan de beheerder/IT-verantwoordelijke instellingen doen in SPF-, DKIM- en/of DMARC-records. In veel gevallen blijkt dit onvoldoende het geval. Dit maakt het voor een cybercrimineel mogelijk om e-mails te verzenden uit naam van een medewerker van jouw bedrijf. Dit wordt ook wel CEO-fraude genoemd. Denk aan een e-mail met een betaalverzoek van de directeur aan de financiële afdeling. Of zelfs een bericht naar klanten/relaties van jouw bedrijf te sturen met het verzoek om een bankrekeningnummer aan te passen.

Veel bedrijven zijn in de veronderstelling dat deze records goed zijn ingericht. Vaak blijkt dat niet alle drie deze records (juist) zijn ingericht. In het verleden was SPF voldoende, snel daarna werd DKIM toegevoegd en sinds een jaar of 5 is DMARC de standaard. Dat is bij veel bedrijven nog onvoldoende bekend dan wel ingericht. Ook bij de instellingen gaat het dan nog wel eens mis. Vaak wordt de policy onjuist ingesteld.

3. E-mailadressen van medewerkers zijn te gemakkelijk vindbaar

E-mailadressen, die zijn toch gemakkelijk te achterhalen voor eenieder en niet spannend als deze publiekelijk bekend zijn? Toch wel, het gaat er namelijk om wat je ermee kunt. Vaak zijn de e-mailadressen namelijk afkomstig uit datalekken. Dan kan ook een wachtwoord bekend zijn.

Ook kan dit gecombineerd worden met informatie over de persoon (op social media) en zijn werkzaamheden/functie/werkgever. Tezamen met het e-mailadres is

het een combinatie die zich uitstekend leent voor cyberaanvallen zoals (spear)phishing en spam-mails. Hierbij geldt de wet van de grote getallen: Hoe meer mailadressen, hoe meer mensen in de fout gaan en klikken op een link. Met alle gevolgen van dien.

In deze databases worden niet alleen e-mailadressen gevonden, maar vaak ook wachtwoorden. Hier kan een cybercrimineel allerlei acties op los laten. Denk aan het doen van inlogpogingen op het bedrijfsnetwerk met veel gebruikte wachtwoorden. Ook dat doet men automatisch, met miljoenen pogingen tegelijkertijd.

Hoe meer e-mailadressen van jouw bedrijf op straat liggen, hoe meer aandacht je zou moeten besteden aan het voorkomen van spam en phishing. Denk aan technische instellingen (spamfilter, e-mailsecurity, ATP) en het opleiden van medewerkers (phishing simulatie testen, awareness trainingen).

4. Websites, vindbare documenten en open poorten spelen cybercriminelen in de kaart

In het onderzoek zijn ook de website, openbare documenten en poorten onder de loep genomen. De belangrijkste conclusies op dit vlak zijn:

- De aanwezigheid van een kwetsbare WordPress website. Het is een veelgebruikte dienst en kent veel mogelijke kwetsbaarheden door achterstallig onderhoud van met name de plug-ins.
- Het publiekelijk beschikbaar zijn van documenten met gevoelige of confidentiële inhoud, waarbij de organisatie vaak niet op de hoogte is dat deze informatie voor het grijpen ligt.
- Open poorten van het bedrijfsnetwerk naar het publieke internet komen vaak voor. Het is echter van belang wat er wordt opengezet en ‘in control’ te zijn. Iets waarvan je niet op de hoogte bent, kun je ook niet beschermen.

Belangrijkste adviezen in het kort:

Er is dus nog veel ruimte voor verbetering. Hieronder zijn de belangrijkste aanbevelingen naar aanleiding van dit onderzoek op een rijtje gezet.

1. Realiseer je hoe gemakkelijk het is informatie en kwetsbaarheden zijn te vinden in openbare bronnen.
2. Zorg ervoor dat je besturingssysteem, je applicaties, netwerkapparatuur en al de overige hardware tijdig wordt voorzien van updates. Breng hiervoor een proces aan naast de managementsoftware die dit kan faciliteren.
3. Zorg voor adequate e-mailbeveiliging, zodat er geen misbruik gemaakt kan worden van jouw bedrijfsdomein. Dit is een heel belangrijk aspect. Het overgrote deel van alle cyberaanvallen begint met phishing.
4. Medewerkers dienen kritisch te zijn op wat zij publiekelijk plaatsen en beschikbaar stellen. Denk hierbij aan gevoelige data of bestanden op een webserver of website.
5. Denk als een hacker. Dat hebben we met dit onderzoek ook gedaan. Organisaties dienen zich te beseffen dat cyberveiligheid verder draagt dan alleen binnen de bedrijfsmuren. Openbare bronnen zijn vaak een ‘blindspot’ en dat moet veranderen om cybercriminelen voor te blijven.

Onderzoeksresultaten

CVE's

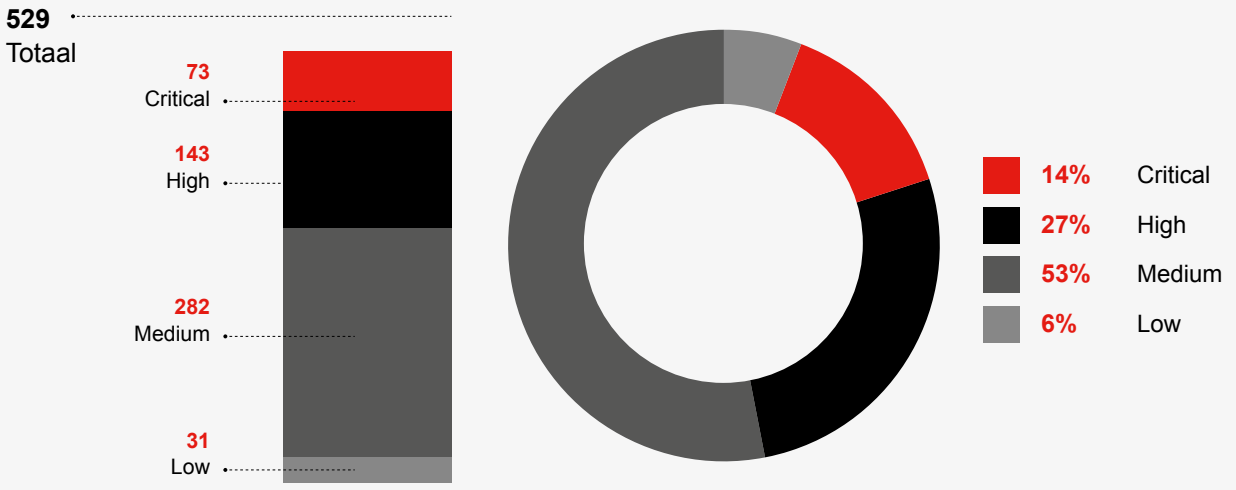
Common Vulnerabilities and Exposures, meestal afgekort als CVE, zijn inzichtelijk in een databank met informatie over kwetsbaarheden in een computersysteem en netwerken. Aan de CVE's wordt een cijfer van 0 tot 10 gekoppeld. Deze cijfers zijn ingedeeld in niveaus: 9 of hoger (=**critical**), 7-9 hoog (=**high**), 5-7 gemiddeld (=**medium**) en 5 en lager (=**low**). Elk niveau geeft de ernst van de CVE weer. Hoe hoger het cijfer, hoe gemakkelijker er misbruik van de kwetsbaarheid kan worden gemaakt.

Score wordt gewaardeerd aan de hand van de impact van de kwetsbaarheid (wat kan met de kwetsbaarheid worden gedaan?) en de kans dat je geïnfecteerd wordt is hoog.

Het doel van een CVE-database is het bijhouden van kwetsbaarheden, zodat men stappen kan ondernemen om systemen en gegevens te beschermen. Door bekende kwetsbaarheden bij te houden, kunnen organisaties en individuen een stap voor blijven op mogelijke bedreigingen en hun systemen en gegevens beschermen tegen indringers.

Bij de onderzochte bedrijven zijn de volgende CVE's geconstateerd:

Verdeling van CVE scores



Bij 64% van de CVE's die als "critical" worden aangemerkt, is bekend hoe deze geëxploiteerd kunnen worden. Daarom is het belangrijk om deze lekken zo snel mogelijk te repareren. Daarmee wordt voorkomen dat jouw bedrijf het doelwit wordt van cyberaanvallen.

Uit het onderzoek blijkt dat 10% van de CVE's ouder is dan 2015. Het is belangrijk om regelmatig te controleren of er nieuwe beveiligingslekken zijn en deze zo snel mogelijk te repareren.

Tot slot blijkt uit de gegevens dat ongeveer 25% van de bedrijven ten minste één Critical CVE heeft. Dit is zeer onwenselijk en een groot risico voor de continuïteit van de organisatie. Het is daarom belangrijk om te controleren of jouw bedrijf zicht heeft op de aanwezigheid van kwetsbaarheden en deze zo snel mogelijk te repareren om te voorkomen dat jouw bedrijf hierdoor het doelwit wordt van cyberaanvallen.

Conclusie

De mogelijke impact van meerdere CVE's is afhankelijk van het aantal en de ernst van de lekken, evenals de manier waarop ze kunnen worden geëxploiteerd.
Over het algemeen kan de aanwezigheid van meerdere bekende beveiligingslekken in een systeem of netwerk de kwetsbaarheid van dat systeem of netwerk verhogen en het risico op cyberaanvallen vergroten.

Het is daarom belangrijk om regelmatig te controleren of er bekende beveiligingslekken zijn en deze zo snel mogelijk te repareren om de beveiliging van het systeem of netwerk te versterken.

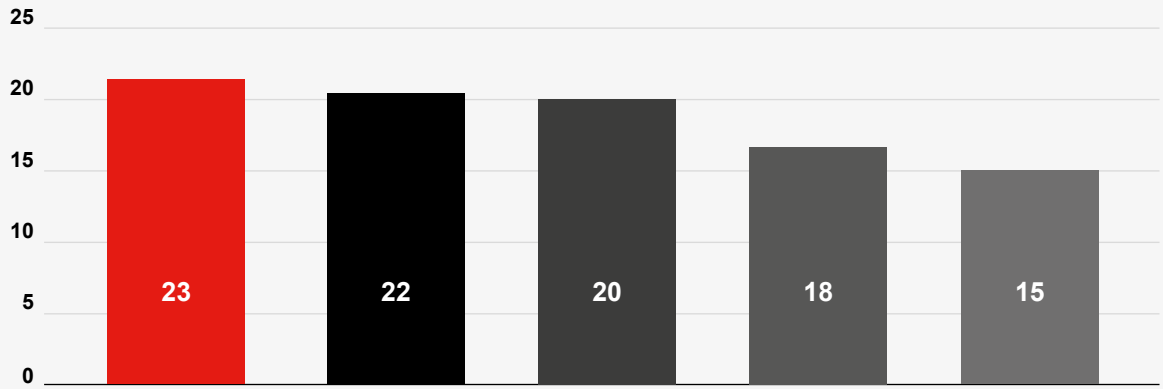
Hoge CVE-cijfers dienen binnen afzienbare tijd opgelost te worden om schade aan systemen en netwerken te voorkomen.

25% van de bedrijven heeft een kritieke CVE

64% van de CVE's heeft een publieke exploit

80,73% van de CVE's is 2 jaar of ouder

Top 5 meest voorkomende CVE's



CVE-2011-3389	CVE-2016-2183	CVE-2016-6329	CVE-2013-0169	CVE-2020-11023
Score: 4.3 (CVSS Version 2.0) Ranking: Medium	Score: 7,5 Ranking: High	Score: 5,9 Ranking: Medium	Score: 2,6 Ranking: Low	Score: 6,1 Ranking: Medium

CVE-2011-3389	Kans om "man-in-the-middle" attack. Iemand kan 2-weg netwerkverkeer onderscheppen en uitlezen.
CVE-2016-2183	Kans op "birthday" attack. Hashes met dezelfde waarde. Sweet32 Attack.
CVE-2016-2183	Kans op "birthday" attack. Hashes met dezelfde waarde. Sweet32 Attack.
CVE-2013-0169	"Side channel" attack. Plain text recovery attack via een statische analyse van timing van gemaakte pakketten aka ''Lucky thirteen".
CVE-2020-11023	Verouderde versie van jQuery. Mogelijkheid om code op te sturen en uit te voeren.

14% van de CVE's heeft de rating critical

12 Juni 2010 OpenSSH 5.6 Oudste CVE

8 Juli 2022 Buffer Overflow Nieuwste CVE

E-mail spoofing

E-mail spoofing is een vorm van cybercrime, waarbij een aanvaller de afzender van een e-mailbericht vervalst om het te laten lijken alsof het afkomstig is van een legitieme bron, met als doel de ontvanger te misleiden en gevoelige informatie te verkrijgen of malware te verspreiden.

Om e-mail spoofing te voorkomen, kunnen de volgende drie methoden worden gebruikt:

1. Sender Policy Framework (SPF)
2. DomainKeys Identified Mail (DKIM)
3. Domain-based Message Authentication, Reporting and Conformance (DMARC)

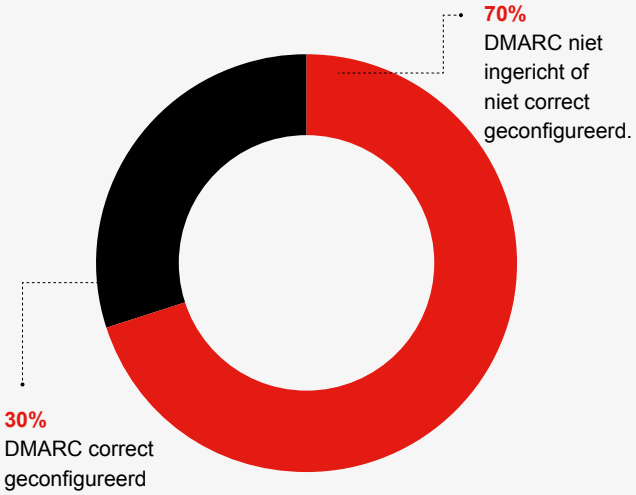
Door SPF, DKIM en DMARC te implementeren en bij te werken, kunnen organisaties de kans op e-mail spoofing aanzienlijk verminderen en hun e-mails betrouwbaarder maken.

Conclusie

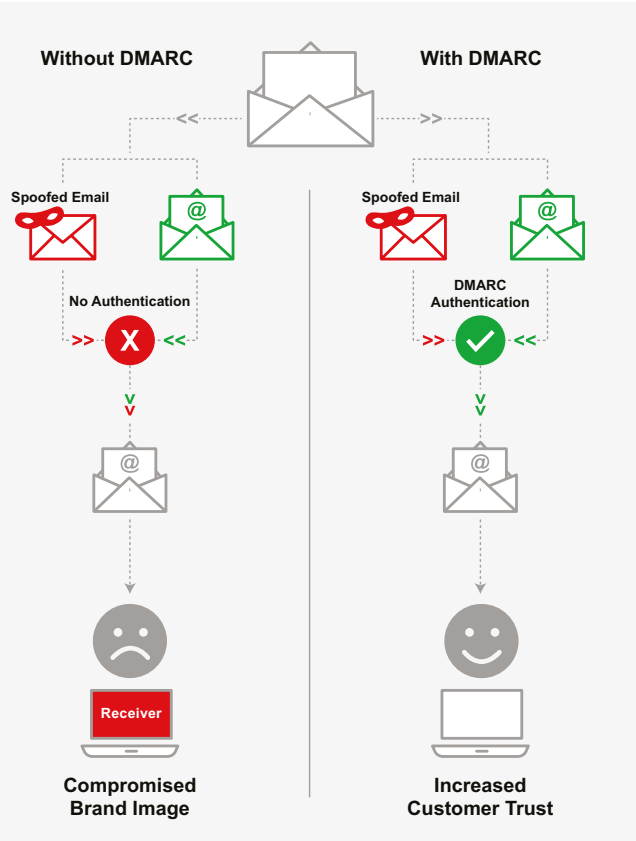
Uit het onderzoek bleek dat 70% van de organisaties geen DMARC-record of geen policy heeft ingeschakeld. Als de policy niet ingeschakeld is, betekent dit dat de policy wel bestaat, maar niet geactiveerd is. Dit is voor de ontvanger hetzelfde als geen DMARC-record, vandaar dat het in de grafiek samen is gevoegd.

Mocht er voor een bepaald domein geen DMARC worden gevonden, houdt dit in dat de verzender geen DMARC-beleid heeft gedefinieerd. In dat geval kunnen e-mails met spam of phishing worden verzonden. Dit is kwetsbaarheid, omdat SPF en DKIM meestal niet voldoende zijn om spoofing te voorkomen. Daarom is het belangrijk —en sterk aan te raden— dat een domeinbeheerder een DMARC-record opstelt voor het domein. Op deze manier kunnen e-mailproviders de authenticiteit van e-mails verifiëren en kan de beveiliging van het domein worden verbeterd.

Hoeveel procent van de onderzoeks-groep zijn vatbaar voor een e-mail spoofing aanval?



Bij 70% van de onderzoeksgroep is DMARC onvolledig of niet geconfigureerd. Dit betekent dat 70% vatbaar is voor spoofing.



Gelekte e-mailadressen

Het lekken van e-mailadressen kan verschillende gevaren met zich meebrengen, waaronder:

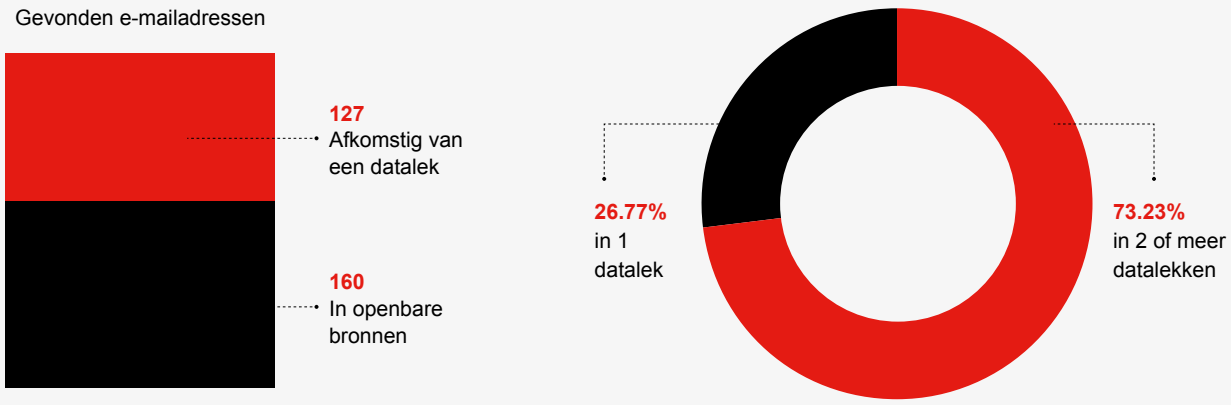
- **Spam:** Wanneer e-mailadressen in handen komen van spammers, kunnen deze adressen worden toegevoegd aan mailinglijsten en kan de ontvanger worden overspoeld met ongewenste e-mails, ook wel spam genoemd.
- **Phishing:** Met behulp van gelekte e-mailadressen kunnen kwaadwillende personen gerichte phishing-e-mails versturen. In deze e-mails wordt geprobeerd om persoonlijke informatie te verkrijgen, zoals wachtwoorden, creditcardgegevens of andere gevoelige informatie.
- **Identiteitsdiefstal:** Wanneer e-mailadressen worden gekoppeld aan andere persoonlijke gegevens, zoals naam, adres of telefoonnummer, kunnen deze worden gebruikt om identiteitsdiefstal te plegen. Met deze gestolen identiteit kan vervolgens fraude worden gepleegd.
- **Reputatieschade:** Als een bedrijf of organisatie e-mailadressen van klanten of medewerkers verliest, kan dit tot reputatieschade leiden. Het kan leiden tot het verlies van vertrouwen van klanten en het imago van het bedrijf kan hierdoor worden beschadigd.

Om deze risico's te vermijden, is het belangrijk om e-mailadressen te beschermen en te zorgen voor een goede beveiliging van persoonlijke gegevens. Dit kan bijvoorbeeld door het gebruik van beveiligde verbindingen en systemen, regelmatige updates van beveiligingssoftware en het goed trainen van medewerkers op het gebied van veilig e-mailgebruik. Ook is het belangrijk om alert te zijn op verdachte e-mails en hier niet zomaar op te reageren of gevoelige informatie te verstrekken.

Conclusie

Op basis van de gevonden informatie is het aantal e-mailadressen van medewerkers in de onderzochte organisaties dat is aangetroffen in datalekken significant. Van alle achterhaalde e-mailadressen is 44,25% in één of meerdere datalekken aangetroffen. Het advies is dan ook om te werken aan het versterken van de beveiliging van e-mailadressen, om het risico op datalekken te verminderen.

Hoeveel e-mailadressen zijn er gevonden op het open-, deep- en darkweb?

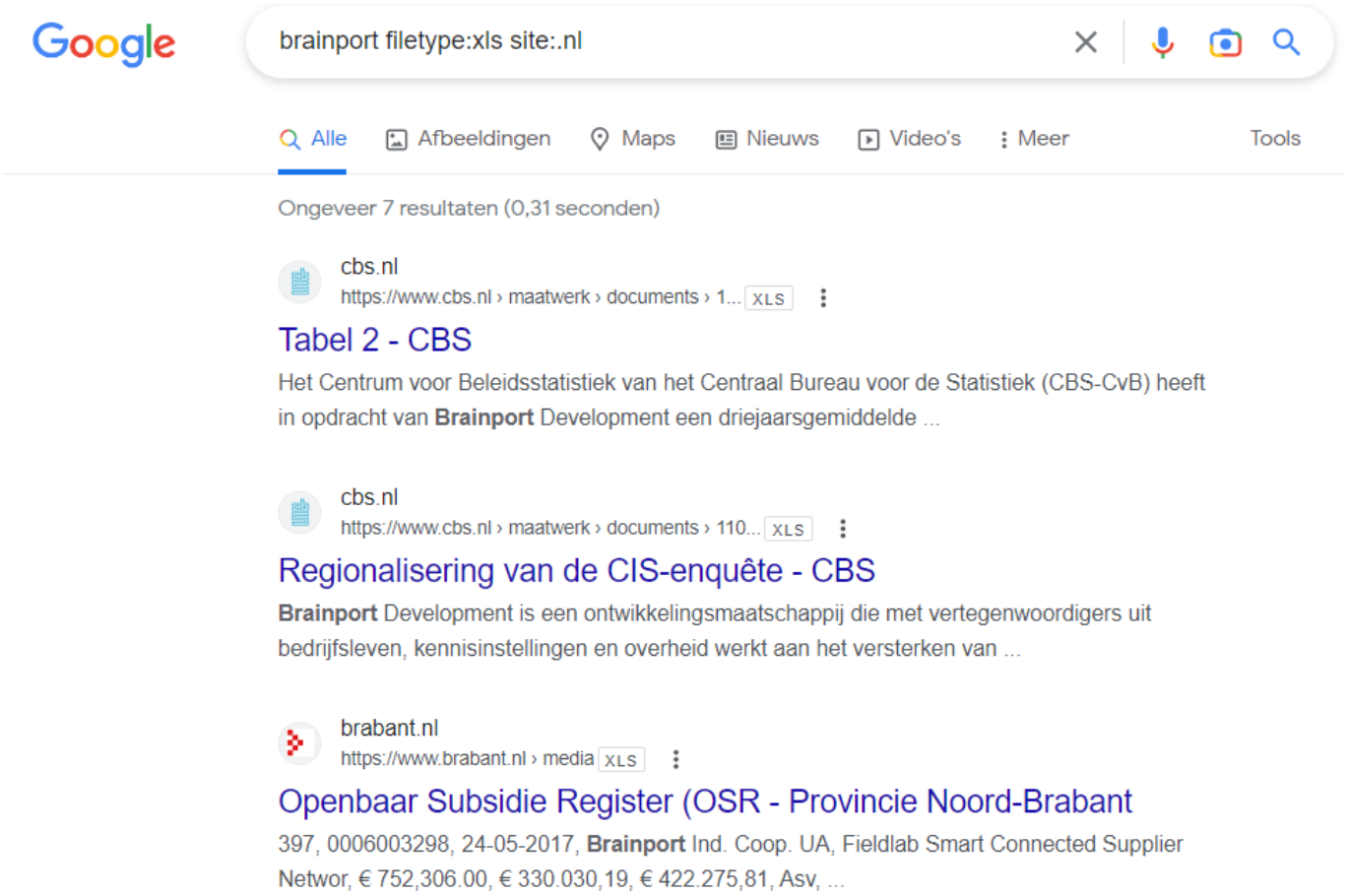


Google Dorking

Google dorking is een zoektechniek, waarbij geavanceerde zoekopdrachten worden gebruikt om informatie te vinden die normaliter niet gemakkelijk gevonden wordt. Denk daarbij aan gevoelige documenten, verborgen pagina's of onbeveiligde databases.

Deze zoektechniek kan zowel voor legitieme als voor niet legitieme doeleinden gebruikt worden, zoals het vinden van kwetsbaarheden in de beveiliging van een website of het ontdekken van gevoelige informatie. Soms wordt dorken gebruikt om informatie te achterhalen die niet openbaar bedoeld is, maar wel voor iedereen toegankelijk is.

Hier is een voorbeeld van een google dork zoekopdracht:



*In dit voorbeeld wordt gezocht naar documenten op Nederlandse domeinen (.nl), waarin Brainport is vermeld, met de specifieke filter op **xls files** (excel bestanden). Op deze manier kan er heel specifiek naar iets gezocht worden met Google.*

Er zijn vier documenttypes (pdf, xls, doc en ppt) onderzocht, omdat deze vaak de meest waardevolle info bevatten. Tot slot is er gezocht op de term ‘admin’. Er zijn van dit bestandstype twee records gevonden binnen de onderzoeksdoelgroep. Deze laatste is van grote waarde, omdat het een pagina kan zijn waar admin-info te vinden is op bijvoorbeeld het CMS van de website of een andere (cloud-)applicatie. De andere documenten kunnen interessante info bevatten, zoals cijfers, klantenbestanden, gebruikersnamen/ wachtwoorden, interne presentaties, businessplannen.

In het onderzoek zijn de volgende standaard dorks gebruikt voor de hele onderzoeksgroep:

- site:”target” file:pdf
- site:”target” file:xls
- site:”target” file:doc
- site: “target” file: ppt
- site:”target”inurl:admin

Na het uitvoeren van Google dorking zijn de volgende resultaten gevonden:

75
Gemiddeld aantal gevonden documenten per bedrijf

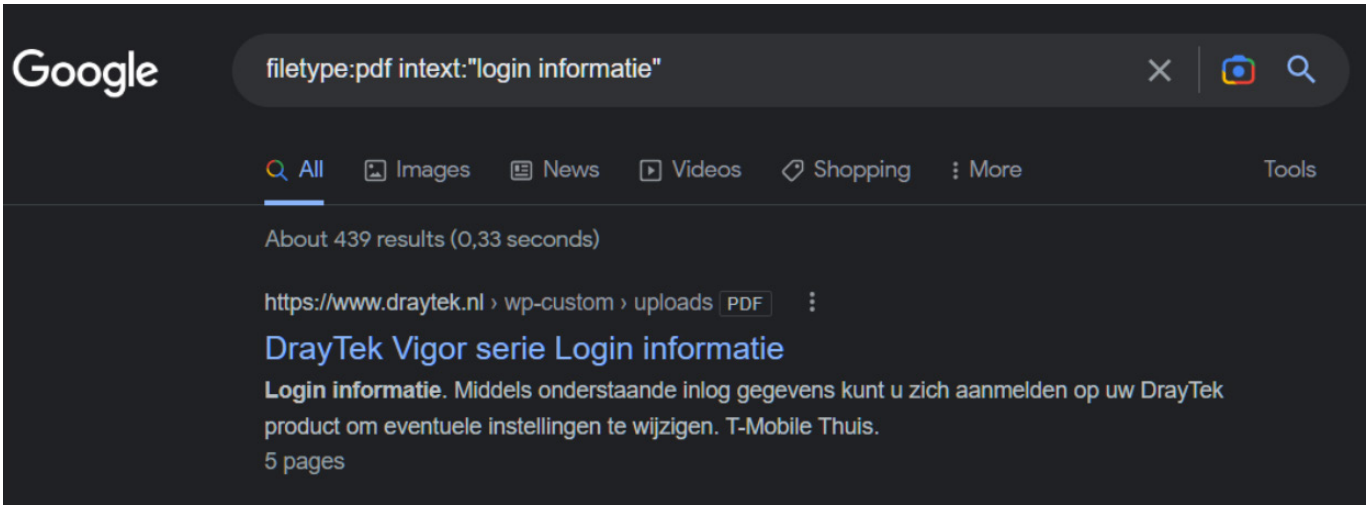
Bij 67% van de bedrijven zijn documenten online gevonden

747*
Hoogste aantal gevonden documenten van één organisatie

** Binnen de onderzoekgroep*

Conclusie

Een van de grootste gevaren van dorking voor een bedrijf is dat het gevoelige informatie kan blootleggen. Een persoon die dorking gebruikt, kan bijvoorbeeld vertrouwelijke documenten, financiële informatie of andere gevoelige gegevens vinden die niet openbaar zouden moeten staan. Dit kan een bedrijf in gevaar brengen voor identiteitsdiefstal, financiële fraude of andere soorten cyberaanvallen.



*Zoals te zien is in het figuur hierboven wordt er gezocht naar **pdf**-files die de woorden ‘login informatie’ bevatten. Met deze zoekopdracht zijn er verschillende inloggegevens gevonden, die niet voor iedereen beschikbaar horen te zijn.*

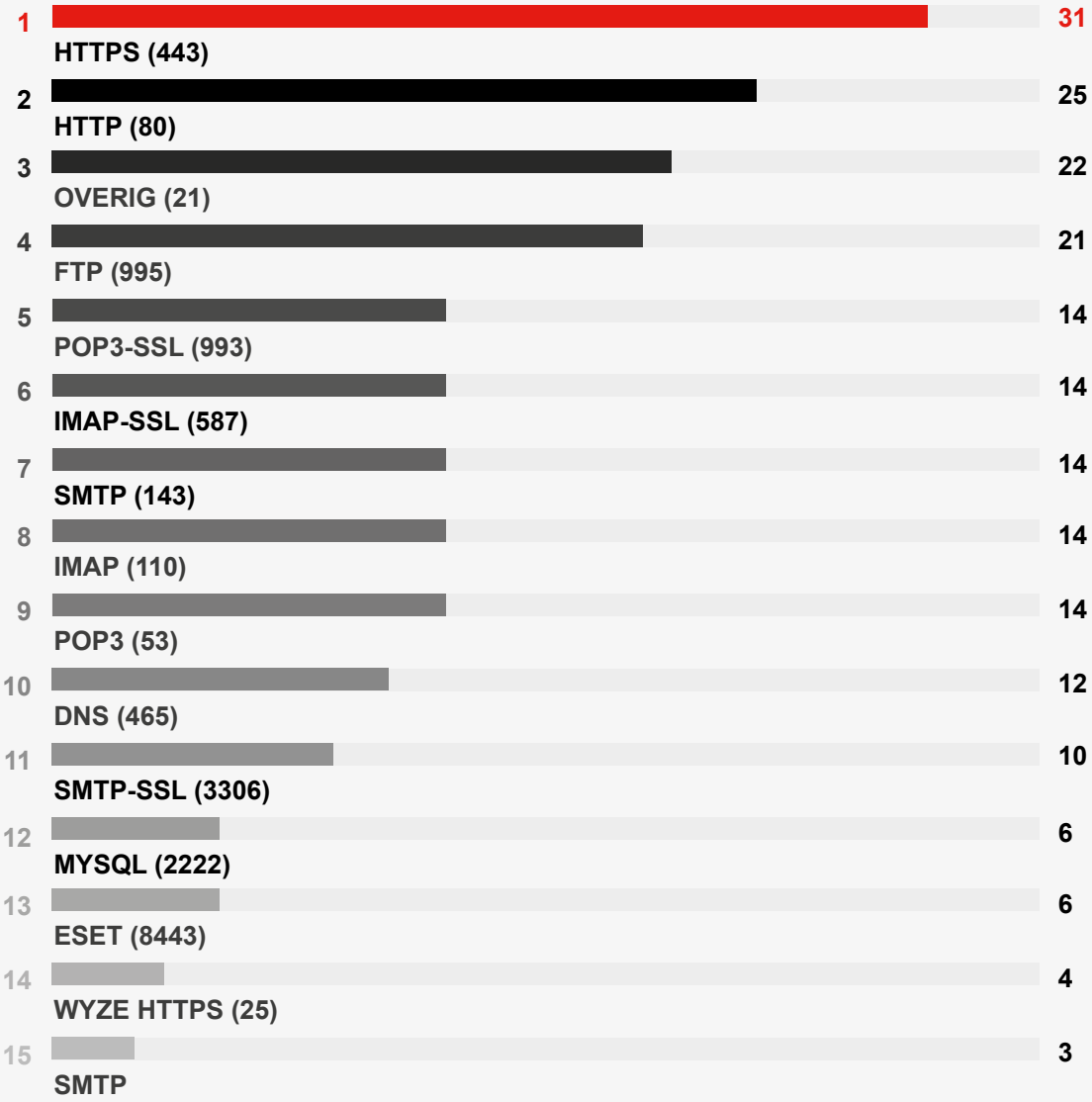
Open poorten

Een **poort** is een connectie binnen het netwerk die een technologie kan beheren. Denk hierbij aan een website, e-mail of een vpn verbinding. Om dit goed te kunnen beheren, hebben deze poorten allemaal verschillende nummers. Deze nummers zijn nodig om de technologieën te onderscheiden.

Er is onderzocht welke poorten en technologieën worden gebruikt binnen de onderzoeksgroep. Het doel van dit soort scans is om te controleren welke poorten open staan en welke technologieën erop draaien.

De poort die in de top 10 opvalt is het ftp-protocol. Dit is een protocol waarbij personen en bedrijven bestanden kunnen delen. Deze technologie vormt een gevaar wanneer deze open staat naar het internet en niet goed beveiligd is. Dit kan leiden tot een cyberaanval op de organisatie.

Welke technologieën (open poorten) werden het meest gevonden?



Binnen de gevonden poort nummers komen er een aantal vreemde poortnummers voor. Dat zijn poorten die niet onder het standaard verkeer vallen richting het internet. Een aantal vreemde poorten die gevonden zijn: **5060**, **5960** en **2091**.

Bij de reguliere poorten, zoals website poorten en e-mail poorten, valt ons op dat er veel ftp-poorten open staan naar het internet. Deze functionaliteit, ondanks redelijk gedateerd, wordt nog steeds gebruikt om bestanden te delen. Deze techniek is, in het licht van huidige dreigingen, niet goed te beveiligen. Er zijn echter beveiligde alternatieven die gebruikt kunnen worden zoals SFTP. De “S” in deze staat voor secure.

Binnen de onderzoeksgroep wordt soms gebruik gemaakt van alternatieve poorten. Denk hierbij aan poort 8443 of 4443. Dit is een alternatieve poort voor het HTTPS verkeer (443). Een andere alternatieve poort is 3390 in plaats van 3389 voor RDP verkeer.

Conclusie

Voordat een hacker een aanval uitvoert, is het gebruikelijk dat hij of zij zoveel mogelijk informatie over het doelwit verzamelt. Dit omvat onder andere informatie over welke poorten open staan en welke technologieën erop draaien. Vervolgens wordt er gekeken of er kwetsbaarheden zijn om te misbruiken.

Als eigenaar van een systeem of netwerk is het daarom belangrijk om potentiële zwakke plekken te identificeren en deze te dichten voordat een hacker er misbruik van kan maken. Dit kan bijvoorbeeld door regelmatig te scannen op open poorten en kwetsbaarheden. Door proactief te zijn in het beveiligen van systemen en netwerken kunnen mogelijke risico's en beveiligingslekken worden verkleind of voorkomen. Tijdens het onderzoek zijn 210 unieke poorten gevonden. Deze poorten gebruiken 35 verschillende technologieën. Gemiddeld staan er 7 poorten open per bedrijf uit de onderzoeksgroep. Het hoogste aantal is 18 open poorten en de organisatie met het minste aantal open poorten, heeft er 2 open staan.

Veelal zijn de technieken File Transfer Protocol (FTP) en Hypertext Transfer Protocol (HTTP) aangetroffen. Dit zijn verouderde technieken en kunnen simpel worden geupgrade naar modernere en veiligere alternatieven zoals SFTP en HTTPS.

Een open poort is niet per definitie een risico. Poort 443 staat bijvoorbeeld vaak open i.v.m. het internetverkeer (http/https). Bij diverse poortnummers kunnen vraagtekens worden gezet en is dieper onderzoek benodigd om de risico's te achterhalen. Het algehele advies is om niet meer poorten open te zetten dan strikt noodzakelijk en periodiek te reviewen of er verouderde technologie wordt gebruikt.

WordPress

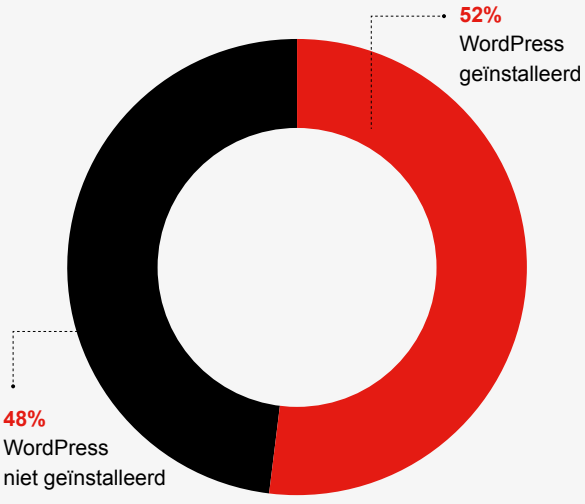
Tijdens het onderzoek is onderzocht welke **Contentmanagementsysteem** (CMS) er gebruikt worden binnen de onderzoeksgroep. WordPress is een van de bekendste CMS-systemen, met een marktaandeel van 43,2% wereldwijd. Binnen de onderzoeksgroep draait 52% een versie van WordPress. Om deze reden is er gekozen om hier onderzoek naar te doen.

Het nadeel van een veel gebruikt CMS is, dat het een makkelijk doelwit is voor hackers, wanneer er online kwetsbaarheden bekend zijn. Hackers proberen via deze bekende kwetsbaarheden toegang te krijgen tot de website en daarmee gevoelige informatie te stelen, de website te defacen, malware te installeren of de website te gebruiken voor phishing- of spam campagnes.

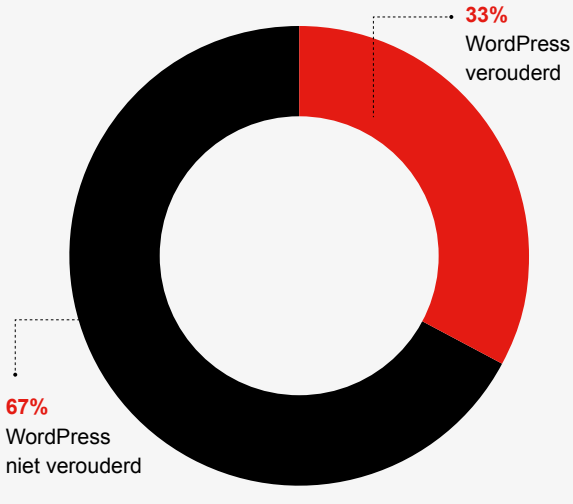
WordPress is een opensource systeem voor het maken van websites. Het wordt wereldwijd veel gebruikt door bedrijven en daardoor is het ook populair onder cybercriminelen. Het is belangrijk om op de laatste versie van de software te zitten. Frequent updaten is dus het advies. Daarbij zijn de plug-ins vaak een nog groter gevaar dan de core-applicatie. Deze plug-ins zijn namelijk van heel veel verschillende leveranciers afkomstig en de kwaliteit loopt zeer uiteen. Ook de webdeveloper is niet altijd een ervaren partij. Daarin schuilt ook een groot risico.

In het onderzoek is er gekeken naar het type CMS, de WordPress versie en de plugin-versie.

Hoeveel procent heeft WordPress geïnstalleerd?



Hoeveel procent van de websites gebruikt een verouderde versie van WordPress?

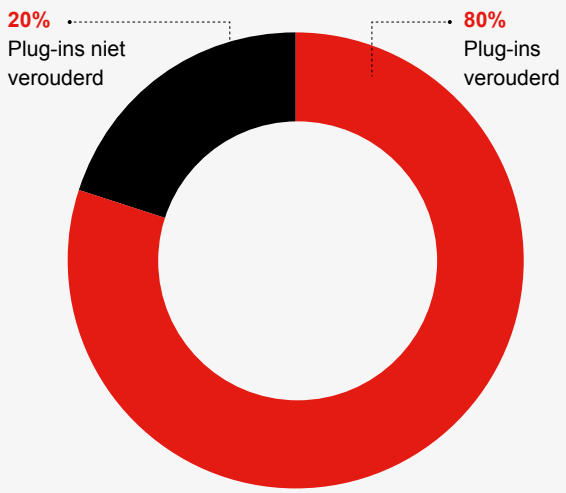


Conclusie

Uit dit onderzoek komt naar voren dat iets meer dan één op de drie WordPress installaties, een verouderde versie is. Ook wordt er gebruik gemaakt van verouderde WordPress plugins. Dit is een risico, omdat oudere versies en plug-ins makkelijker te misbruiken zijn.
Wat verder opvalt bij het onderzoek is dat meer dan 60% van de onderzochte WordPress websites gebruik maakt van een verouderd communicatieprotocol genaamd XML-RPC. Het wordt door verscheidene security instanties geadviseerd om waar nodig en mogelijk over te stappen naar beter beveiligde protocollen.

Tip: Het is belangrijk om een CMS up-to-date te houden en regelmatig te controleren op mogelijke kwetsbaarheden en beveiligingsproblemen. Daarnaast is aan te raden bedrijven hun WordPress versie en de bijbehorende plug-ins updaten.

Percentage WordPress websites met minimaal 1 plugin die verouderd is



Over ACA IT-Solutions

ACA IT-Solutions is gespecialiseerd in dienstverlening en advisering op het gebied van IT en cybersecurity. Daarbij hechten wij veel waarde aan de kracht van samenwerking. Wij staan namelijk graag aan de zijde van de ondernemer om samen te kijken naar de best passende oplossing voor de organisatie en die is steeds anders: anders ten opzichte van andere organisaties en anders in de loop der tijd.

ACA IT-Solutions is, met ruim 30 jaar ervaring, een betrouwbare IT-partner voor veel verschillende typen organisaties voor het MKB, grootbedrijf en instanties. De werkzaamheden bestaan o.a. uit het leveren van advies, ontwerp, installatie, ondersteuning, beheer en trainingen op ICT-gebied. Meer informatie: **aca-it.nl**

Cyber-assessment

In de vraagstelling en onderzoeksaanpak van dit marktonderzoek en de hierop volgende OSINT-scan komen elementen terug uit de cybersecurity assessments die ACA IT-Solutions uitvoert voor opdrachtgevers. Meer informatie over deze assessments en onze werkwijze is terug te vinden op **aca-it.nl/scan**

Vragen of contact

Voor vragen over de onderzoeksopzet, de resultaten en/of advies over dit marktonderzoek kan contact opgenomen worden met:

ACA IT-Solutions
Beukenlaan 40-50
5651 CD Eindhoven
040-8800100
info@aca-it.nl