Cybersecurity binnen Familiebedrijven

Benchmark Cybersecurity websites

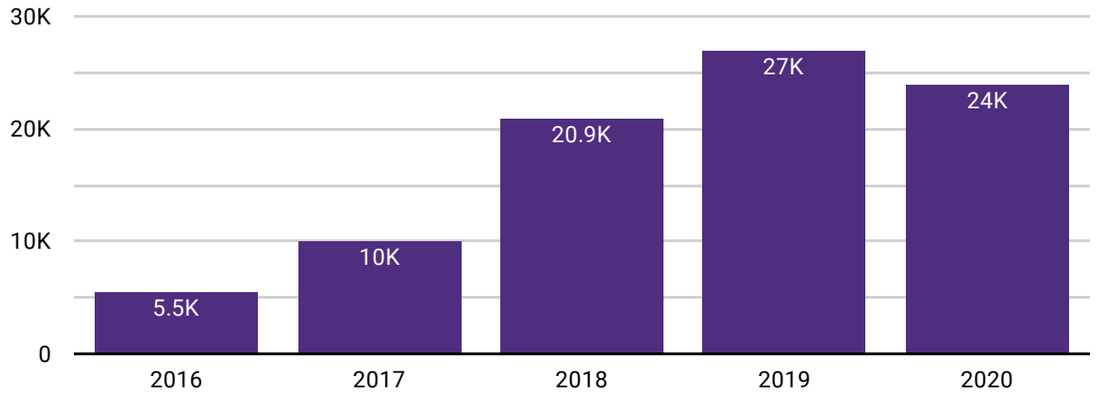
Maart 2022

Cyberincidenten vormen een substantieel risico voor een onderneming. Niet alleen op financieel gebied maar zeker ook qua imago en reputatieschade. Een hack legt niet alleen uw processen stil, maar kan ook voor korte of langere tijd de hele keten verlammen. Het afgelopen jaar maakten verschillende incidenten duidelijk wat de impact van een digitale storing of aanval is. De Log4j en Microsoft Exchange kwetsbaarheden zijn recente voorbeelden hiervan. De cyberoorlog in Oekraïne laat zien welke gevolgen dergelijke cyberaanvallen meebrengen.

De technologische vernieuwingen binnen alle bedrijven nemen ook een vlucht. Denk aan automatisering, data gestuurde technologie en supply chain management. Dat is nodig om ook in de toekomst een effectieve bedrijfsvoering te garanderen

Technologische innovatie wordt breder toepasbaar en beschikbaar. Onze maatschappij is in grote mate afhankelijk van digitale processen en analoge terugvalopties bij uitval zijn er vaak niet. Met alle gevolgen van dien.

Datalekken per jaar



Bron: Autoriteit Persoonsgegevens (AP)

Slechte informatiebeveiliging kan verstrekkende gevolgen hebben. Naast financiële consequenties krijgt u door cybercriminaliteit ook te maken met het verlies van klantgegevens, het dalend vertrouwen van klanten en soms zelfs het tijdelijk stilvallen van de onderneming en alles wat daarmee samenhangt in de keten.

Maar niet alleen cybercriminaliteit vraagt om aandacht voor informatiebeveiliging. Ook het strengere toezicht zoals de Algemene Verordening Gegevensbescherming (AVG) is een belangrijke reden om uw zaken goed op orde te hebben.

Resultaten benchmark beveiliging websites familiebedrijven

Uw website is het visitekaartje van uw onderneming en bevat informatie over uw producten en diensten. De online etalage van uw onderneming is vaak 24/7 benaderbaar voor klanten, maar ook voor hackers. Weet u eigenlijk hoe veilig uw website is?

De praktijk laat zien dat hackers steeds slimmer worden om toegang te krijgen tot (klant)gegevens. En als uw website niet veilig is, hoe is het dan gesteld met de gehele cyberweerbaarheid van uw onderneming?

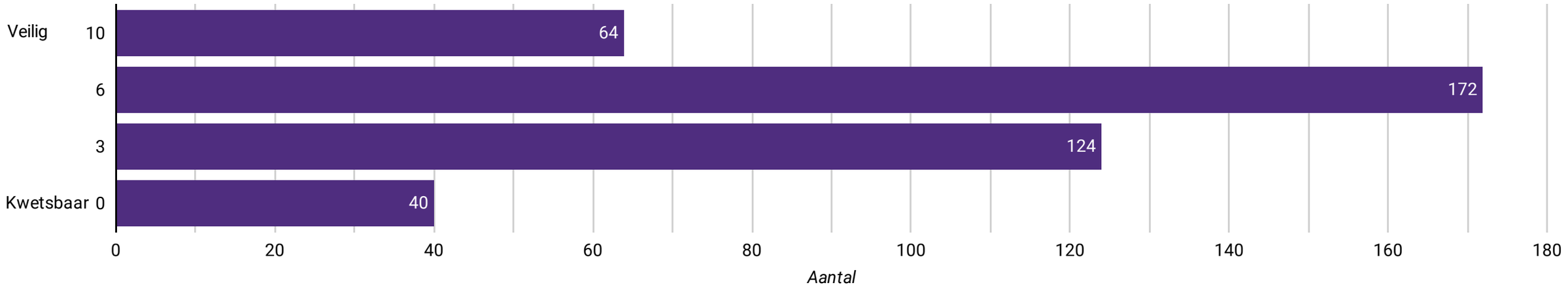
Wij onderzochten de veiligheid van websites van de familiebedrijven binnen Nederland. De gemiddelde cyberweerbaarheidsscore van deze websites is uitgekomen op een 5.5. 164 organisaties scoorde een onvoldoende (score lager dan 6). Op de volgende pagina's leest u de resultaten per hoofdgebied.

Aanpak

Voor deze benchmark analyseerden wij 400 sites van de familiebedrijven binnen Nederland. We onderzochten 9 typen beveiligingskwetsbaarheden, verdeeld over 3 hoofd categorieën: het systeem, het beheer en de gegevens.

Wij maken gebruik van openbare informatie. Onze geavanceerde CyberHunter tool scant websites met een beperkte set aan tests. Wij garanderen u dat geen aanvallen zijn uitgevoerd op de websites om de beveiliging te testen.

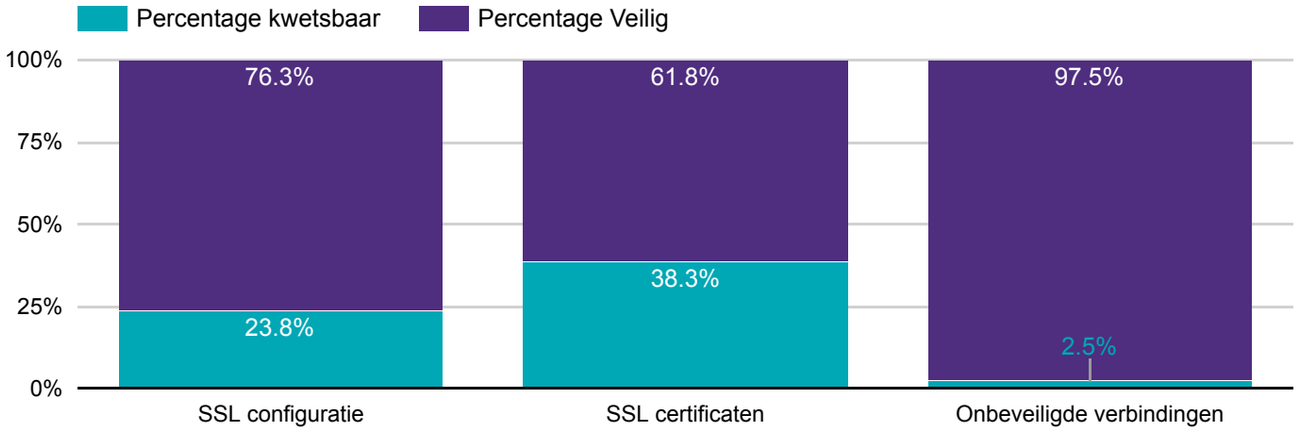
Gemiddelde score beveiliging websites



Hoe veilig zijn de gegevens?

Bezoekers van website laten vaak (persoonlijke) gegevens achter, bijvoorbeeld via het contactformulier. Dat moet op een veilige manier gebeuren zodat hackers ze niet kunnen onderscheppen.

Uit ons onderzoek blijkt dat 38,3% van de websites kwetsbare SSL certificaten heeft. Daarentegen heeft slechts 2,5% van de websites nog geen beveiligde verbinding (SSL). Van de websites die wel een beveiligde verbinding hebben, bevat 23,8% een onveilige (SSL) configuratie van de versleutelde verbinding.



SSL Configuratie

Met een beveiligde (SSL) verbinding, kan data versleuteld worden verstuurd.

Maar niet elke beveiligde (SSL) verbinding is even veilig. Zo voldoet ook niet elk deurslot aan het politiekeurmerk.

Een onveilige SSL configuratie maakt het voor aanvallers makkelijker om in de beveiligde verbinding te breken, net als bij een onveilig slot, met als mogelijk gevolg dat gevoelige informatie lekt.

SSL certificaten

SSL certificaten zijn vereist voor het opzetten van een beveiligde verbinding. Ze zorgen ervoor dat (gevoelige) gegevens aankomen bij de juiste partij op een veilige manier.

Een SSL certificaat is te vergelijken met een paspoortcontrole. Met het paspoort stel je de identiteit vast van een persoon.

Problemen met het certificaat zorgen ervoor dat de geldigheid van de website niet vastgesteld kan worden. Dat leidt mogelijk tot het lekken van gegevens van de bezoeker. Het certificaat heeft een beperkte houdbaarheid en moet periodiek opnieuw uitgegeven worden door een betrouwbare derde partij.

Onbeveiligde verbindingen

Data veilig over het internet versturen kan via een SSL verbinding.

Zonder een beveiligde (SSL) verbinding kunnen (gevoelige) gegevens onderschept worden door een aanvaller.

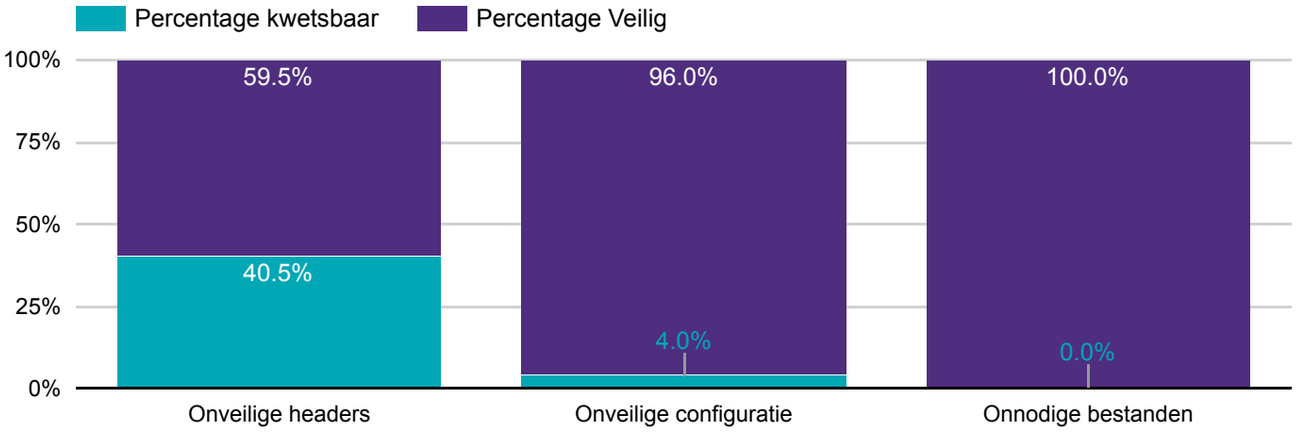
Een onbeveiligde verbinding is te vergelijken met het schreeuwen van je wachtwoord in een vol voetbalstadion, iedereen in de buurt kan dit horen.

Hoe veilig is het systeem?

Om een website aan te bieden op het internet is een onderliggende infrastructuur met systemen nodig (hosting).

Uit het onderzoek komt naar voren dat het merendeel (96%) van deze systemen veilig geconfigureerd zijn en geen onnodige bestanden bevatten.

Met de aanvullende bescherming is het slechter gesteld: 40,5% van deze systemen biedt geen aanvullende bescherming voor bezoekers, door het niet ondersteunen van security 'headers'.



Onveilige headers

De website kan aanvullende informatie meegeven aan de browser van de gebruiker. Deze informatie bevat gegevens over hoe de website veilig bezocht kan worden door de browser.

De browser slaat deze informatie op in "headers". Zo kan een header informatie bevatten over hoe lang gegevens bewaard moeten worden in de browser. Ook helpen deze headers voor extra beveiliging tegen aanvallers.

Hoe beter deze headers zijn ingesteld, hoe veiliger het bezoeken van de website wordt.

Onveilige configuratie

Technische gegevens over de website en onderliggende infrastructuur worden zichtbaar voor het publiek als de webserver onveilig geconfigureerd is.

Denk aan versienummers van de gebruikte software of informatie over hoe de website geconfigureerd is.

Deze informatie geeft een mogelijke aanvaller inzicht in de gebruikte technologie. Zo zoekt en test hij of zij naar kwetsbaarheden om toegang te krijgen tot het systeem.

Onnodige bestanden

Websites kunnen bestanden aanbieden aan gebruikers (bijvoorbeeld een brochure). De beheerder van de website kan bepalen welke bestanden toegankelijk wordt voor iedereen via het Internet.

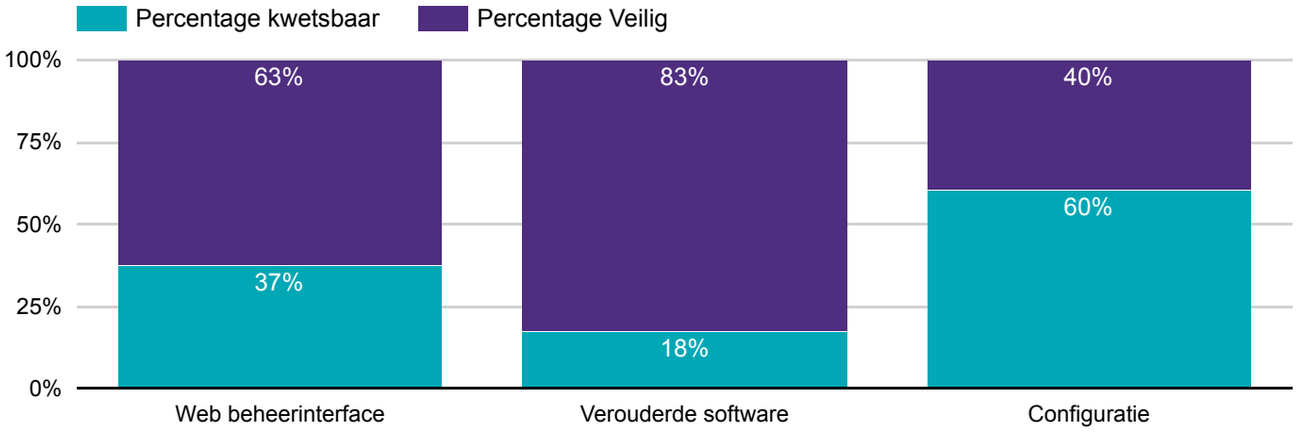
Maar soms worden gevoelige bestanden ongewenst zichtbaar voor iedereen. Denk aan back-ups en andere bestanden die een eindgebruiker nooit mag zien.

Mogelijk gevoelige documenten komen zo beschikbaar via internet.

Hoe veilig is het beheer?

De website en de onderliggende infrastructuur (hosting) moet op een veilige manier beheerd en onderhouden worden.

Meer dan de helft (60%) van de websites van familiebedrijven bevatten kwetsbaarheden in de configuratie van de webserver. 37% van de websites heeft een kwetsbare beheerinterface, waardoor ongewenste ingangen (zoals interfaces voor beheer van de website) publiekelijk toegankelijk zijn voor aanvallers.
Daarnaast bevat 18% van de websites verouderde en daarmee mogelijk kwetsbare software.



Web beheerinterface

Veel websites maken gebruik van standaard softwarepakketten zoals Wordpress of Joomla. Met deze software beheert men de website op afstand de website, bijvoorbeeld voor het aanpassen van teksten.

De beheerinterface (plek om in te loggen) van deze software is vaak publiekelijk toegankelijk voor iedereen en dus niet alleen voor de beheerders.

Aanvallers kunnen proberen om de gebruikersnaam en het wachtwoord te raden van deze beheerinterface, om zo toegang te krijgen tot de website bijvoorbeeld om de website aan te passen.

Verouderde software

De website en de onderliggende infrastructuur (hosting) maakt gebruik van software.

Verouderde software kan kwetsbaarheden bevatten die aanvallers graag uitproberen als ingang om binnen te komen.

Afhankelijk van de kwetsbaarheden kan dit dus ernstige gevolgen hebben.

Configuratie

De onderliggende infrastructuur van websites bevatten vaak (onnodige) ingangen die gebruikt worden om de omgeving te beheren. Aanvallers proberen via deze ingangen in te loggen en daarmee vormen ze een risico.

Slaagt een aanvaller erin om toegang te krijgen, dan zijn zij in staat om de website onbereikbaar te maken of de inhoud van de website aan te passen.

Hoe veilig is uw website

Bent u benieuwd naar de veiligheid van uw website? Vraag dan nu kosteloos de Cyber website scan aan. U ontvangt binnen 24 uur een overzichtelijk rapport waarin u zelf ziet hoe uw website presteert ten opzichte van de benchmark van de overige leden.

Ik wil inzicht

Cyber risk services helpt u op weg naar basisveiligheid
Het scannen van uw website is een eerste stap maar voor een gedegen cyberweerbaarheid is meer nodig. Er is géén snelle manier om een bedrijf cyberweerbaar te maken. Het vergt een grondige aanpak en raakt veel processen. Daar helpen we u graag bij.

Met onze pragmatische Cyberweerbaarheidscheck weet u snel waar de knelpunten van cybersecurity binnen uw onderneming zitten. Samen met u bekijken we welke maatregelen nodig zijn om de cyberweerbaarheid te vergroten. Zo helpen we bijvoorbeeld bij het opstellen van een informatiebeveiligingsplan inclusief een plan hoe te handelen bij een cyberaanval.

We kiezen daarbij altijd voor de meest pragmatische oplossing die goed bij uw onderneming past. En natuurlijk ondersteunen we bij de implementatie van de maatregelen als dat gewenst is.

Niets is belangrijker dan veilig ondernemen. Kijk voor meer informatie op:

grantthornton.nl/veiligondernemen

Grant Thornton

Wilt u meer weten? Neem dan contact op:

Migiel de Wit-Beets
Partner Cyber risk services
T 088 676 91 86
E migiel.de.wit@nl.gt.com