VARONIS

RAPPORT GEGEVENSRISICO'S 2021

GEZONDHEIDSZORG, FARMACEUTISCHE BEDRIJVEN EN BIOTECH

De gemiddelde gezondheidswerker heeft op de eerste werkdag toegang tot **31.000 vertrouwelijke bestanden**.

INHOUD

VARONIS

OVER HET RAPPORT

Het Rapport gegevensrisico's 2021 is het tweede rapport van onze jaarlijkse serie over sectorspecifieke bedreigingen, trends en oplossingen.

Dit rapport richt zich op gegevensbeveiliging in de gezondheidszorg: ziekenhuizen, farmaceutische ondernemingen en biotechnologiebedrijven. Voor het rapport werden meer dan 3 miljard bestanden van 58 organisaties geanalyseerd.

Veel van onze bevindingen worden verder uitgesplitst per bedrijfsgrootte:

- **Klein:** tot 500 werknemers
- **Middelgroot:** 501–1500 werknemers
- **Groot:** meer dan 1500 werknemers

Dit rapport heeft als doel organisaties in zorg- en biotechsector meer inzicht te geven in de kwetsbaarheden van hun cyberbeveiliging met het oog op toenemende bedreigingen, en biedt tips voor zorgorganisaties om toekomstige risico's te beperken.

Opgesteld op basis van gegevensanalyse van **3 miljard bestanden** van **58 zorgorganisaties**

Ziekenhuizen

Farmaceutische bedrijven

Biotech

VARONIS

BELANGRIJKSTE BEVINDINGEN

COVID-19 vormde vruchtbare grond voor aanvallers om verwarring te zaaien en misbruik te maken van zorgorganisaties in de frontlinie. Van ziekenhuizen die dag en nacht patiënten onderzochten tot farmaceutische bedrijven die geavanceerde vaccins ontwikkelden; cybercriminelen richtten zich op organisaties en systemen die onder enorme druk stonden.

Aanvallen op de zorg- en biotechsector geven blijk van een ongekende mate van kwaadwilligheid. De methoden variëren, maar het doel blijft hetzelfde: toegang krijgen tot vertrouwelijke gegevens en deze stelen, doorverkopen of gebruiken om mensen af te persen.

In 2020 bestookten cybercriminelen honderden ziekenhuizen met krachtige varianten van ransomware als Maze en Ryuk. Door de overheid gefinancierde actoren richtten zich op farma- en biotechbedrijven om gegevens over COVID-19-onderzoek te bemachtigen. Bedreigingen van binnenuit bleven druk leggen op de zorgsector en door simpele menselijke fouten werden vertrouwelijke gegevens niet beveiligd. Dat zorgde voor extra risico in een toch al problematisch jaar. 2020 was ook het eerste jaar waarin de dood van een patiënt rechtstreeks kon worden teruggevoerd op een cyberaanval.

Met zo veel op het spel, wilden we inzicht krijgen in de mate waarin de zorg- en biotechsector vertrouwelijke informatie beveiligt. Het blijkt dat de sectoren nog heel wat te doen hebben: we ontdekten dat **elke medewerker toegang heeft tot één op de vijf bestanden.**[1]

Door onvoldoende gegevensbeveiliging in combinatie met een toegenomen aantal aanvallen die steeds verfijnder worden, **is de gezondheidszorg een van de sectoren die in 2021 de grootste risico's loopt.**

[1] In dit rapport verwijst “iedereen” naar elke werknemer van de organisatie.

VARONIS

Gezondheidszorg Belangrijkste bevindingen

Bijna 20% van alle bestanden is toegankelijk voor alle werknemers van een zorgorganisatie (gemiddeld)

31.000 vertrouwelijke bestanden (HIPAA + financieel + eigen onderzoek) zijn **toegankelijk voor iedereen**

Meer dan **50% van de organisaties heeft** meer dan **1000 vertrouwelijke bestanden** die toegankelijk zijn voor **alle werknemers**

Circa **twee derde van de organisaties** heeft meer dan **500 accounts met wachtwoorden die nooit verlopen**

ALGEMENE BEVINDINGEN

De gezondheidszorg is onvoldoende voorbereid op de toename van bedreigingen in de sector

Blootstelling per organisatiegrootte

Organisatiegrootte	Gem. aant. bestanden	Gem. aant. bestanden toegankelijk voor iedereen	Gem. % bestanden toegankelijk voor iedereen
Groot	62.470.271	10.872.986	16%
middel	49.177.666	12.767.695	23%
Klein	16.686.926	4.617.693	25%
Gemiddeld	**54.270.776**	**11.160.270**	**19%**

Organisatiegrootte	Gem. aant. mappen	Gem. aant. mappen toegankelijk voor iedereen	Gem. % mappen toegankelijk voor iedereen
Groot	4.742.019	887.009	16%
middel	3.259.977	820.933	23%
Klein	608.652	178.044	25%
Gemiddeld	**3.894.805**	**813.052**	**19%**

Organisatiegrootte	Gem. aant. vertrouwelijke bestanden	Gem. aant. vertrouwelijke bestanden toegankelijk voor iedereen	Gem. % vertrouwelijke bestanden toegankelijk voor iedereen
Groot	473.215	34.435	11%
middel	220.034	20.970	14%
Klein	132.763	57.930	22%
Gemiddeld	**353.701**	**30.948**	**12%**

Gemiddeld heeft elke werknemer toegang tot meer dan 11 miljoen bestanden — bijna 20% van het totale aantal bestanden van de organisatie. Maar in kleine en middelgrote bedrijven hebben **werknemers vrij toegang tot bijna één op de vier bestanden.**

Organisatiebrede blootstelling van medische persoonsgegevens en intellectueel eigendom vormt een reëel risico. **Gemiddeld is meer dan 1 op de 10 vertrouwelijke bestanden toegankelijk voor elke werknemer.**

Vergeleken met financiële dienstverleners heeft de gemiddelde zorg- of biotechorganisatie ongeveer 75% minder gegevens. Maar hoewel zorgorganisaties minder bestanden hebben, hebben ze **een groter aantal bestanden dat toegankelijk is voor alle werknemers.** Aanvallers die erin slagen toegang te krijgen tot één geautoriseerd apparaat, kunnen toegang krijgen tot de hele organisatie of enorme hoeveelheden gegevens coderen met ransomware.

ALGEMENE BEVINDINGEN

Staat van gegevens per terabyte: gezondheidszorg

Organisatie-grootte	Bestanden	Mappen	Bloot-gestelde mappen	Bloot-gestelde bestanden	Mappen met unieke machtigingen	Bloot-gestelde vertrouwe-lijke bestanden	Verlopen vertrouwe-lijke bestanden	Niet opgeloste SID's[2]	Mappen met inconsistente machtigingen	Aantal geanaly-seerde rapporten	TB geanaly-seerd per bedrijf
Groot	1.550.171	157.569	33.457	13.108	12.587	993	8136	999	1497	32	52
middel	1.716.089	178.935	28.091	19.611	11.330	1966	13.114	1348	1003	22	45
Klein	919.923	51.774	10.888	11.888	10.474	5107	6425	502	851	4	56
Gemiddeld	**1.569.640**	**158.377**	**29.865**	**15.490**	**11.965**	**1646**	**9906**	**1097**	**1265**	**58**	**50**

De gemiddelde terabyte bestaat uit 1,3 miljoen bestanden. Gemiddeld 2% daarvan (20.000 bestanden) bevat vertrouwelijke informatie, zoals patiëntgegevens, eigen onderzoek en persoonsgegevens. Het risico per terabyte geeft een duidelijker beeld van de gemiddelde kwetsbaarheid voor aanvallen per organisatiegrootte en laat zien welke organisaties het meest kwetsbaar zijn voor bedreigingen van binnenuit en van buitenaf.

We ontdekten dat kleinere organisaties een stuitende hoeveelheid blootgestelde gegevens hebben, waaronder vertrouwelijke bestanden, intellectueel eigendom en patiëntgegevens. Op hun eerste dag hebben nieuwe werknemers van kleine bedrijven **direct toegang tot meer dan 11.000 blootgestelde bestanden, waarvan bijna de helft vertrouwelijke gegevens bevatten.** Hierdoor ontstaat een enorme kwetsbaarheid voor aanvallen en neemt het risico op non-conformiteit in het geval van datalekken toe.

Bij grotere organisaties zaten de problemen voornamelijk in de bevoegdhedenstructuren, waardoor het risico op datalekken door cyberaanvallen toeneemt.

[2] Onopgeloste SID's (beveiligings-ID's) ontstaan wanneer een account op een toegangsbeheerlijst wordt verwijderd uit AD. Onopgeloste SID's zorgen voor complexiteit en kunnen worden misbruikt.

ALGEMENE BEVINDINGEN

Zorggegevens beveiligen

Bedrijven met vertrouwelijke bestanden toegankelijk voor alle werknemers via algemene toegang

Vertrouwelijke bestanden toegankelijk voor iedereen	% bedrijven
< 1000	45%
1000-10.000	22%
> 10.000	33%

Niet gebruikte vertrouwelijke gegevens per grootte van bedrijf in de zorgsector

Grootte van het bedrijf	Gem. aant. niet gebruikte vertrouwelijke bestanden	Gem. % vertrouwelijke bestanden die niet gebruikt worden
Groot	258.288	67%
middel	146.609	67%
Klein	70.980	72%
Sectorgemiddelde	**245.826**	**69%**

Via algemene toegangsgroepen (bijvoorbeeld Iedereen, Domeingebruikers, Geautoriseerde gebruikers) kunnen gebruikers binnen een organisatie informatie delen. Wanneer gegevens te eenvoudig toegankelijk zijn en onvoldoende worden beveiligd, kunnen organisaties snel de controle kwijtraken; werknemers kopiëren, delen, verwijderen en wijzigen zelfs de meest vertrouwelijke gegevens. Onbeveiligde informatie is een gemakkelijk doelwit voor cybercriminelen; zij hoeven slechts één eindgebruiker te hacken om een voet tussen de deur te krijgen in uw omgeving.

Zorgverleners en onderzoekers moeten informatie die wordt beschermd door verschillende verordeningen, zoals de Health Insurane Portability and Accountability Act (HIPAA) in de VS en de AVG in de EU, daadkrachtig beschermen. Organisaties die zich niet houden aan de HIPAA-regels en zich niet inspannen om vertrouwelijke patiëntgegevens te beveiligen, kunnen **een boete krijgen tot wel $ 1,5 miljoen per jaar.** Bedrijven die niet voldoen aan de AVG, kunnen een boete krijgen tot **€ 20 miljoen of 4% van hun jaaromzet.**

Bij ruim de helft van de ziekenhuizen, farmaceutische bedrijven en biotech-ondernemingen zijn meer dan 1000 vertrouwelijke bestanden blootgesteld aan alle werknemers. **Bij een derde van de organisaties die we onderzochten, zijn meer dan 10.000 bestanden toegankelijk voor alle werknemers.** Beheer op basis van minimale bevoegdheden is een basisstap die elke organisatie kan nemen om gegevens te beschermen tegen diefstal, om misbruik te voorkomen en om te zorgen voor naleving van verordeningen.

ALGEMENE BEVINDINGEN

Alleen geautoriseerd personeel: kwetsbaarheden in Active Directory

Bedrijven met wachtwoorden die niet verlopen

Wachtwoorden die niet verlopen	% bedrijven
< 500	23%
500-1500	36%
> 1500	41%

Bedrijven met spookgebruikers

Omvang van groep met verlopen gebruikersaccounts	% bedrijven
< 1000	21%
1000-10.000	57%
> 10.000	22%

"Spookgebruiker": gebruikers- en serviceaccounts die inactief zijn, maar nog wel bestaan. Zij vormen voor hackers een eenvoudige manier om ongemerkt door de bestandsstructuren van een organisatie te gaan. Hackers maken vaak misbruik van deze kwetsbaarheid om gegevens te stelen of kritieke systemen te verstoren.

Uit gegevensanalyse door Varonis blijkt dat de zorgsector ver onder het gemiddelde scoort voor wat betreft het opsporen en oplossen van deze kwetsbaarheid. **77% van de bedrijven die we onderzochten, heeft 501 of meer accounts met wachtwoorden die nooit verlopen en heeft 79% meer dan 1000 spookgebruikers.**

DE STATUS VAN DE SECTOR

Als 2020 een voorteken is van wat de toekomst ons brengt, nemen cyberaanvallen op de zorgsector alleen maar toe.

Medische professionals bereikten COVID-19-vaccinatiemijlpalen met ongekende snelheid, maar intussen nam het aantal bevestigde datalekken ook toe met een schrikbarende 58% omdat kwaadwillende actoren zich richtten op vaccinonderzoek en intellectueel eigendom met hoge prioriteit.

De sector was bijzonder slecht voorbereid op deze aanvallen. Slechts 23% van de zorgorganisaties maakt gebruik van geautomatiseerde beveiliging. Het resultaat: een datalek heeft een gemiddelde levenscyclus van 329 dagen — de hoogste score van alle sectoren — en de gemiddelde **kosten per datalek bedroegen in 2020 $ 7,13** miljoen — een toename van 10,5% ten opzichte van 2019.

Cyberaanvallen waren ook verfijnder dan in de voorgaande jaren. Neem bijvoorbeeld de wereldwijde inbraakcampagne waarbij updates van de Orion-bedrijfssoftware van SolarWinds een Trojaans paard bevatten om een nieuw soort malware genaamd SUNBURST te verspreiden. Deze aanval heeft nog altijd wijdverbreide gevolgen en is nog steeds van invloed op overheden, adviesbureaus, technologie- en telecombedrijven.

Om de steeds schadelijkere en verfijndere cyberaanvallen voor te zijn, moeten ziekenhuizen, farmaceutische bedrijven en biotech-ondernemingen zich meer gaan richten op het ontwikkelen van hun beveiliging en procedures in geval van incidenten. Beheer met minimale rechten, beveiliging van vertrouwelijke gegevens en beperking van laterale bewegingen in hun omgeving zijn de absolute minimale voorzorgsmaatregelen die zorgorganisaties moeten treffen.

De gemiddelde kosten van een datalek in de zorgsector bedroegen **$ 7,13 miljoen in 2020.**

CASESTUDY

Hoe Varonis een top 20-spoedkliniek helpt beveiligingsincidenten snel en adequaat op te lossen

Toen een insider snel achter elkaar 15.000 bestanden opende, had Chris maar enkele minuten om uit te zoeken of zijn bedrijf werd aangevallen en de aanval te stoppen voordat deze leidde tot een datalek.

Ontdek hoe Varonis helpt.

DOWNLOAD DE VOLLEDIGE CASESTUDY

VARONIS

OVER VARONIS

Varonis is een pionier in gegevensbeveiliging en analyses, gespecialiseerd in software voor gegevensbeveiliging, bedreigingsdetectie en reactie, en compliance. Varonis beschermt bedrijfsgegevens en cyberaanvallen door gegevensactiviteit, perimetertelemetrie en gebruikersgedrag te analyseren; voorkomt catastrofes door gevoelige gegevens te vergrendelen; en garandeert de veiligheid dankzij automatisering.

Door onze primaire fileserver gaan en die beveiligen zoals Varonis doet — daar zou ik met mijn hele team jaren mee bezig zijn, en zelfs dan zou het ons niet lukken."

CHRIS M.
Systems Engineer

Benieuwd hoe **uw organisatie** het doet?

Ontvang een gratis evaluatie van uw gegevensrisico door Varonis. Ontdek verborgen risico's voor uw belangrijkste gegevens - snel en zonder extra werk op uw bord.

CONTACT OPNEMEN

Vertrouwd door