Bescherm online informatie bij de overheid

Overheden zijn constant het doelwit van hackers. Aangezien overheidsinstanties met zeer gevoelige informatie werken, is de keuze niet meer OF maar HOE de veiligheid van digitale communicatie binnen de overheid te verbeteren.

Dit document geeft een overzicht van het huidige cybersecurity landschap. Tevens geven we handvatten om te bepalen welke van de beschikbare communicatieplatforms voldoen aan de veiligheidsstandaarden voor de overheid.



Veroorzaakte Schade Cybercriminaliteit

$6 biljoen / jaar



113 Overheids Agentschappen

waren het slachtoffer van ransomware aanvallen in 2019

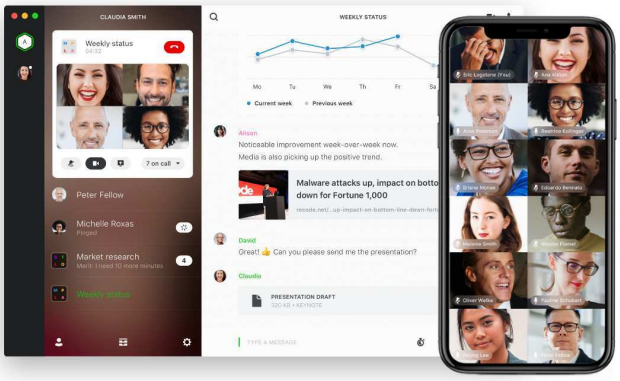
Wereldwijd waargenomen risico's in 2020*

Economie	Risico 1	Risico 2	Risico 3
Amerika	Cyberaanvallen	Verspreiding van besmettelijke ziektes	Data fraude en diefstal
Canada	Cyberaanvallen	Verspreiding van besmettelijke ziektes	Werkloosheid
England	Cyberaanvallen	Fiscale crisis	Extreme Weersomstandigheden
Duitsland	Cyberaanvallen	Onvrijwillige migratie	Activa Bubbel
Nederland	Cyberaanvallen	Verspreiding van besmettelijke ziektes	Falen aanpassen aan klimaatverandering

* Gegevens verzameld door het World Economic Forum om te bepalen waar het bedrijfsleven van de wereld zich het komende decennium het meest zorgen over maakt.

Volgens het 'Risks For Doing Business' rapport uit 2020 van het World Economic Forum staat Cyberaanvallen op de derde plaats in de wereldwijde top risico's voor organisaties.

In o.a. in England, Duitsland, Canada, de VS en Nederland worden cyberaanvallen als de grootste zorg beschouwd. Meer dan ooit tevoren moeten organisaties het beschermen van online informatie prioriteren. Ze moeten overwegen wat wel en niet bijdraagt aan het beschermen van hun informatie.



> Wire was the clear choice as a partner - not only is their collaboration platform secured with the highest level of end-to-end encryption, they are built upon principles of transparency and privacy that many others lack.
>
> Tomas Nystrom, IT Director at Fortum.

Over Wire™

Wire is het meest veilige samenwerkingsplatform en transformeert de manier waarop bedrijven communiceren. Dit doet zij met dezelfde snelheid waarmee onze oprichters telefonie met Skype hebben getransformeerd. Met het hoofdkantoor in Berlijn en kantoren in Zwitserland en San Francisco, telt Wire's erkende samenwerkings- en communicatieplatform meer dan 1.800 zakelijke klanten wereldwijd. Wire wordt door IDC, Forrester en Gartner erkend als een van de veiligste samenwerkingsplatforms en biedt messaging, audio- / videoconferenties, het delen van bestanden en externe samenwerking - allemaal beschermd door de sterkste end-to-end-versleuteling.

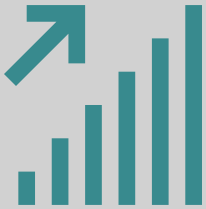
Bezoek wire.com voor meer informatie over Wire's veilige communicatieoplossing gericht op overheden

Prijswinnende Keuze

Vertrouwd door onze Partners

De 5 belangrijkste security onderdelen van Een communicatie infrastructuur

In een digitale architectuur waar veiligheid prioriteit nummer 1 is wordt alles onder de loep genomen en geverifieerd middels de modernste beveiligingsprotocollen op basis van zero trust. Dit betekent dat digitale communicatie een vergelijkbaar veiligheids- en privacy-niveau zou moeten hebben als een persoonlijk gesprek.



COVID-19 heeft geresulteerd in dat werknemers gebombardeerd worden met gehaaide cyberaanvallen met steeds realistischere imitaties van hackers die zich voordoen als erkende overheidsinstanties. FBI-gegevens stellen dat **cyberaanvallen tijdens de pandemie met 400% zijn toegenomen.**

1. De Allernieuwste Versleuteling

End-to-End-Encryption (E2EE) is niet langer een add-on, het is een fundamentele noodzaak voor veilige communicatie. Maar niet alle end-to-end-encryption is op dezelfde manier gemaakt. Door **voorwaartse en achterwaartse geheimhouding** te gebruiken, wordt elk bericht afzonderlijk versleuteld in plaats van voor alles één sleutel te gebruiken. Het is gebleken dat sommige protocollen veiliger zijn dan anderen. Een gedecentraliseerde oplossing die **double-ratchet E2EE** gebruikt zorgt ervoor dat elk individueel gesprek, bericht en bestand afzonderlijk op elk apparaat kan worden versleuteld. Hierbij worden de sleutels gegenereerd vanaf het apparaat in plaats van uit een centrale server. Dit beschermt de informatie tot de kleinst mogelijke eenheid. Hierdoor wordt er een systeem gecreëerd dat alsmaar complexer (en daardoor moeilijker om te hacken) wordt naarmate het groeit.

2. Data Soevereiniteit

Data is cruciaal in elke branche, nog wel belangrijker voor overheidsorganisaties, waarbij de druk enorm en de dreigingen complex zijn. Organisaties moeten prioriteit geven aan data soevereiniteit door een **zero-trust-beleid** te implementeren. Dit kan door systemen die data uitwisselen of hosten te verplaatsen naar **een private cloud of lokaal te hosten.**

3. Continuïteit van de dienstverlening

Een cruciaal element is de mogelijkheid dat in het geval het netwerk aangevallen is/wordt om hierover te kunnen blijven communiceren. Organisaties **moeten een veilige omgeving bieden voor kritieke-/crisiscommunicatie**, anders zullen medewerkers hun eigen manieren vinden om te communiceren. Dit zal resulteren in dat potentieel vertrouwelijke en gevoelige informatie onbedoeld blootgesteld zou worden aan derden. Beveiligings- en afweer protocollen kunnen zo aan het licht komen. Dit brengt de organisatie in onomkeerbaar gevaar. En hierbij worden de significante boetes, die kunnen volgen bij het niet naleven van regelgeving, nog buiten beschouwing gelaten.

4. Beveiliging van Federation & Messaging Layer

Wire™ leidt de ontwikkeling van een nieuwe, wereldwijde open standaard voor veilige communicatietechnologieën genaamd Messaging Layer Security (MLS).

In samenwerking met marktleiders is het doel van Wire om een **veilig, interoperabel en federatief systeem te creëren waarmee gebruikers tussen verschillende berichten systemen kunnen werken met hetzelfde niveau van privacy en beveiliging dat Wire biedt.** Alan Duric, medeoprichter van Wire en Skype Alumnus, hielp eerder bij de ontwikkeling van WebRTC en leidt de ontwikkeling t.a.v. MLS. Dit zal zorgen voor een bredere standaard voor alle vormen van communicatie versleuteling.

Federatie is vooral belangrijk voor overheidsafdelingen om met elkaar te kunnen communiceren via hun eigen intranet en tegelijkertijd veilig te blijven.

5. Ultra-transparantie

Organisaties die bescherming van online informatie prioriteren zullen zien dat beveiliging, privacy en transparantie hand in hand gaan. Er is geen beveiliging als privacy geschonden wordt. **De beste manier om echte privacy te garanderen is door middel van open-source code**. Open source laat zien dat een leverancier echt gefocust is op het nemen van een proactieve en een minder ondoorzichtige benadering bij het delen van zijn beveiligingsmaatregelen, waarbij audits van de software door derden mogelijk gemaakt dienen te worden.

Door de mogelijkheid te hebben om de broncode van de technologie te onderzoeken, kan er precies bepaalt worden hoe de leverancier omgaat met gegevens, integraties, opslag van encryptiesleutels en andere mogelijke oorzaken van beveiligingsrisico's.

Het kiezen van veilige Online Communicatie

Door het toenemende aanbod van communicatie en samenwerking oplossing, kan het lastig zijn om te kiezen. Hieronder vindt men richtlijnen speciaal voor overheidsorganisaties om zo het risico van cybercriminaliteit te minimaliseren.

Vergelijking van Communicatie Oplossingen*

	E2EE Text	E2EE Audio	E2EE Video	E2EE Bestanden Delen	E2EE Scherm Delen	Open-source Code	Gecertificeerde Dienst
Wire	✓	✓	✓	✓	✓	✓	FedRAMP In Progress
Cisco Webex	✓	✓	✓	✓	✓	X	FedRAMP
Dust	✓	n.v.t.	n.v.t.	n.v.t.	n.v.t.	X	None
Google G Suite	X	X	X	X	X	X	FedRAMP
GoToMeeting	✓	✓	✓	n.v.t.	n.v.t.	X	None
Jitsi Meet	✓	✓	✓	✓	✓	✓	None
Mattermost	X	X	X	n.v.t.	X	✓	None
Microsoft Teams	X	X	X	X	X	X	FedRAMP
Signal	✓	✓	n.v.t.	✓	n.v.t.	✓	None
Skype For Business	X	X	X	X	X	X	FedRAMP
Slack	X	X	X	X	X	X	FedRAMP
WhatsApp	✓	n.v.t.	✓	✓	n.v.t.	X	None
Wickr	✓	✓	✓	✓	✓	✓	None
Zoom	✓	X	X	✓	X	X	FedRAMP

Legenda: n.v.t. = niet van toepassing

* De data is gebaseerd op een NSA cybersecurity rapport - “selecting and safely using collaboration services for telework”

Waarom Wire de juiste partner is voor overheidsorganisaties

Overheidsorganisaties gebruiken Wire zodat zij controle houden over gevoelige informatie. En tevens om werknemers een veilig communicatiekanaal te bieden. Of ze nu thuis, onderweg of in het buitenland zijn, gebruikers kunnen direct en veilig audio- en videogesprekken voeren, berichten verzenden en bestanden delen.

Gemaakt Voor Geclassificeerde Omgevingen



INSTALLATIE OP LOCATIE / OFFLINE	RELEASE RECOMMENDATION FROM BSI
FEDERATION	DOOR DERDEN GECONTROLEERD
100% OPEN-SOURCE CODE	VOLDOENEND AAN GDPR/CCPA

Gebouwd om essentiële mobiele communicatie te beschermen. Wire's beveiliging is uniek erkend door de IDC.

Hoe de Duitse overheid Wire gebruikt

Met een groot aantal thuiswerkende Duitse overheidsmedewerkers werd de bescherming van gevoelige communicatie buiten de eigen IT-firewalls cruciaal.

De Duitse overheid gebruikt Wire om het werken vanaf elke locatie te vergemakkelijken en daarbij de veiligheidsrisico's hiervan drastisch te verlagen. Het federale bureau voor beveiliging van informatietechnologie *(Bundesamt für Sicherheit in der Informationstechnik - BSI)* heeft een vrijgave advies uitgebracht voor de beveiliging die Wire biedt. Momenteel is het de enige officiële online dienst voor het verwerken van geclassificeerde informatie bij de Duitse overheid.

Uitmuntende Veiligheid

- Aanbevolen door de NSA en BSI
- Perfecte voor-/achterwaartse geheimhouding
- Militair veiligheidsniveau
- Minimaal gebruik van metadata
- Ontwikkeld door oud-Skype oprichters

Rijk aan functionaliteiten

- Volledig samenwerkingsoplossing
- Aanpasbare ephemeral berichten
- Veilige externe gastenkamers
- 25 audio- en 12 video gesprekken
- Werkt met een lage bandbreedte

Gebruiksvriendelijk

Wire heeft een strak en intuïtief ontwerp dat gewaardeerd wordt door gebruikers. Het is net zo gebruiksvriendelijk als applicaties die je privé gebruikt en is beschikbaar op iOS, Android, Windows, Mac en Webapp.

Wereldwijd vertrouwd door overheden, ministeries en defensies



Beschermen van essentiële gevoelige informatie



Beschermen tegen cyber-spionage



Veilig Mobiel Communiceren



Onmiddellijk reageren op incidenten

Wire Enterprise

Geheel aanpasbaar lokaal gehost platform voor veilige communicatie voor de gehele organisatie. Verzeker ervan dat communicatie voldoet aan de hoogste veiligheidsstandaarden.

Neem Contact Op

Wire Pro

Een End-to-end versleuteld SaaS platform. Creëer een account, nodig collega's uit, en start in een paar minuten veiliger te communiceren en samen te werken.

Neem Contact Op