

## Nieuws



## CISA: blokkeer uitgaande RDP-verbindingen naar externe netwerken

vrijdag 1 november 2024, 10:01 door [Redactie](#), 2 [reacties](#)

De Amerikaanse overheid **adviseert** organisaties om uitgaande RDP-verbindingen naar externe of publieke netwerken te verbieden of drastisch te beperken. "Deze maatregel is cruciaal om blootstelling aan mogelijke cyberdreigingen te beperken", aldus het Cybersecurity and Infrastructure Security Agency (CISA) van het Amerikaanse ministerie van Homeland Security.

Aanleiding voor het advies van de overheidsinstantie is een **grootschalige phishingaanval** waarbij gebruik wordt gemaakt van RDP-configuratiebestanden. Doelwitten ontvangen een e-mail met een .rdp-bestand. Wanneer de ontvanger het bestand opent maakt zijn computer verbinding met de RDP-server van de aanvaller. Via het Remote Desktop Protocol (RDP) is het mogelijk om op afstand toegang tot computers te krijgen.

Zodra de computer van het doelwit verbinding met de RDP-server van de aanvallers maakt, kunnen die allerlei vertrouwelijke gegevens en bestanden stelen en proberen verdere aanvallen uit te voeren. Volgens het CISA is het dan ook belangrijk dat organisaties RDP-bestanden in e-mailclients en webmaildiensten blokkeren. Daarnaast moeten organisaties maatregelen nemen om te voorkomen dat gebruikers RDP-bestanden kunnen openen, wat het CISA een zeer belangrijke voorzorgsmaatregel noemt om de kans op misbruik tegen te gaan.

Organisaties worden ook aangeraden om naar ongeautoriseerde uitgaande RDP-verbindingen te zoeken die het laatste jaar zijn opgezet. Tevens krijgen organisaties het advies om gebruikers te onderwijzen. "Robuuste gebruikerseducatie kan helpen om de dreiging van social engineering en phishingmails tegen te gaan. Bedrijven zouden een educatieprogramma moeten hebben dat duidelijk maakt hoe verdachte e-mails zijn te herkennen en rapporteren."

- ▲ Microsoft waarschuwt voor password spraying door botnet van TP-Link-routers
- ▼ Aanvallers maken actief misbruik van lekken in PTZ-beveiligingscamera's

## Reacties (2)

Vandaag, 11:16 door [Anoniem](#)

[Reageer met quote](#) 

Beheerder: mooi, poort 3389 uitgaand geblokkeerd  
We zijn veilig.

Aanvaller: \*stuurt rdp file met :443 in het adres \*

Vandaag, 11:27 door [wim-bart](#)

[Reageer met quote](#) 

*Door Anoniem:* Beheerder: mooi, poort 3389 uitgaand geblokkeerd  
We zijn veilig.

Aanvaller: \*stuurt rdp file met :443 in het adres \*

Daarom afdwingen dat RDP altijd via een RDP gateway gaat. Dit kan met GPO's. Vervolgens alleen de gateway toestaan via authenticatie toestaan en de firewall van de gateway beperkten tot toegestane adressen. Je kan ook nog gateway profielen maken om dit te regelen op basis van groep lidmaatschap bijvoorbeeld naar welke RDP end hosts je kan verbinden.

## Reageren

Ondersteunde bbcodes

Je bent niet [ingelogd](#) en reageert "[Anoniem](#)". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je [hier direct een account aanmaken](#). Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.



[Nieuwe code](#)

Herhaal code:

[Preview](#)

[Reageren](#)

Zoeken



## Wintertijd:

- ☐ Body says yes
- ☐ Body says no
- ☐ Anders:

Aantal stemmen: **910** [43 reacties](#)

## Vacature



### Chief Information Security Officer

Utrecht heeft jou nodig! Als Chief Information Security Officer speel jij een cruciale rol in de bescherming van de digitale informatie van de gemeente Utrecht. Als geen ander weet jij welke dreigingen er zijn en kun je deze vertalen naar risico's die de gemeente en haar inwoners lopen. Solliciteer nu!

[Lees meer](#) 

De GGD heeft mij voor deelname aan de Gezondheidsmonitor uitgenodigd. Mag dit wel zonder mijn toestemming?

**30-10-2024** door [Arnoud Engelfriet](#)

Juridische vraag: Ik kreeg een brief om mee te doen aan de GGD Gezondheidsmonitor, een onderzoek in opdracht van de GGD. Hierin ...


[Lees meer](#)  [17 reacties](#)

## Vacature



### Cybersecurity Trainer / Streamer

Toe aan een nieuwe nieuwe job waarmee je het verschil maakt? In de Certified Secure trainingen laat je deelnemers zien hoe actuele kwetsbaarheden structureel verholpen worden. Ook werk je actief mee aan de ontwikkeling van onze gamified security challenges. Bij het maken van challenges kom je telkens nieuwe technieken tegen, van Flutter tot GraphQL, van Elastic Search tot Kubernetes.

[Lees meer](#) 

## Proton mail backup

**24-10-2024** door [Ase2004](#)

Ik denk dat de meeste gebruikers van Proton (mail) zich niet realiseren dat ze hun userdata niet backuppen. Dit betekent dus ...

[Lees meer](#)  [22 reacties](#)



## Security.NL - X

**10-01-2024** door [Redactie](#)

Altijd meteen op de hoogte van het laatste security nieuws? Volg ons ook op X!

[Lees meer](#) 