Van: **Digital Trust Center** <algemeen@digitaltrustcenter.nl>
Aan:
Onderwerp: [DTC Informatiedienst #17548] Voorbeeld notificatie RDP service
Datum: 23.08.2022 10:05:37 (+02:00)

digital trust center.

Ministerie van Economische Zaken en Klimaat

This notification is meant for Dutch companies and those who conduct commercial activities in the Netherlands

Notificatie kwetsbaarheid RDP service [DTC]

Geachte heer, mevrouw,

Namens het Digital Trust Center (DTC), onderdeel van het ministerie van Economische Zaken en Klimaat, attenderen wij u op een mogelijke cybersecuritydreiging voor uw bedrijf. Dit blijkt uit actuele dreigingsdata waar we over beschikken [1].

Het betreft de volgende cybersecuritydreiging:

Een op het internet aangesloten systeem dat te herleiden is naar uw organisatie, is (mogelijk) verkeerd geconfigureerd. Het gaat om een Remote Desktop (RDP) service die bereikbaar is via het publieke internet en dus door iedereen te benaderen. Hierdoor kan een kwaadwillende (mogelijk) toegang verkrijgen tot gevoelige informatie over de IT-infrastructuur. De RDP-service is via het int ernet te bereiken op poort 3389 (TCP) [1].

Vanuit de bron Shadowserver [1] hebben wij vernomen dat u kwetsbaar bent voor deze dreiging op de volgende IP adres(sen):

{'ip': '255.255.255.255', 'hostname': 'domein1234.nl'}

De afgelopen jaren zien onderzoekers een toename van het aantal RDP-services die publiek benaderbaar zijn vanaf het internet om bijvoorbeeld het thuiswerken te faciliteren. Tegelijk zijn dit soort services een groot doelwit voor cybercriminelen en waarschuwt de FBI voor ransomware die via kwetsbare RDP-configuraties wordt uitgerold [2].

Wat kunt u doen?

• Voorkom dat het RDP-protocol direct benaderbaar is via het internet. Zorg dat gebruikers eerst een VPN-verbinding maken naar het bedrijfsnetwerk en sta RDP verbindingen alleen over deze VPN-verbinding toe.
• Zorg dat alleen sterke en unieke wachtwoorden worden gebruikt en stel een limiet in na hoeveel foute inlogpogingen een gebruikersaccount wordt geblokkeerd. Denk hierbij bijvoorbeeld aan 10 keer zodat een “brute force” aanval niet mogelijk is.
• Maak waar mogelijk gebruik van tweefactorauthenticatie. Sta hier stil bij de gekozen inrichting. Configureer dit bijvoorbeeld op de VPN-verbinding en/of op de computer of server waarnaar je wilt verbinden via RDP.
• Houd je computers en servers up-to-date. Stel beveiligingsupdates voor systemen die via RDP benaderbaar zijn niet uit maar voer deze zo snel

mogelijk door.
• Neem contact op met uw IT-dienstverlener als u hierop zelf geen actie kunt ondernemen.
• Bezoek onze website voor aanvullende informatie en maatregelen die u kunt treffen [3].

Twijfelt u aan dit bericht? Bezoek onze overheidswebsite en lees hoe u de betrouwbaarheid van het Digital Trust Center als afzender kunt valideren [4].

Graag vernemen wij of dit bericht nuttig voor u was [5].

Wij hopen u hiermee voldoende te hebben geïnformeerd om de dreiging op te lossen. Indien u al bekend was met deze dreiging en al actie ondernomen heeft, kunt u deze mail als niet verzonden beschouwen. Mocht u nog vragen hebben, dan kunt u op deze e-mail reageren.

[1] https://www.shadowserver.org/what-we-do/network-reporting/accessible-rdp-report/
[2] https://www.security.nl/posting/759150/FBI+waarschuwt+voor+ransomware+die+organisaties+via+rdp+binnendringt
[3] https://www.digitaltrustcenter.nl/rdp
[4] https://www.digitaltrustcenter.nl/controle
[5] https://www.digitaltrustcenter.nl/feedback-notificatie

Met vriendelijke groet,
Operator Digital Trust Center (DTC)

.....
www.digitaltrustcenter.nl
algemeen@digitaltrustcenter.nl
+31 70 379 67 00
Postbus 20401 | 2500 EK | Den Haag
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
.....

DTC privacyverklaring

De privacyverklaring van het Digital Trust Center (DTC) vindt u op de onderstaande website.
https://www.digitaltrustcenter.nl/privacy