



Nieuws



## Plastisch chirurgische kliniek lekt patiëntgegevens bij RDP-bruteforce-aanval

vrijdag 1 november 2024, 11:54 door Redactie, 0 reacties

Een plastisch chirurgische kliniek in de Verenigde Staten heeft de gegevens van meer dan tienduizend patiënten gelekt, nadat aanvallers door middel van een RDP-bruteforce-aanval toegang tot systemen wisten te krijgen. Vervolgens werd er ransomware uitgerold. De kliniek en het Amerikaanse ministerie van Volksgezondheid zijn nu een schikking van **500.000 dollar** overeengekomen.

De aanval deed zich in juli 2017 voor. De aanvallers wisten via een bruteforce-aanval op een RDP (Remote Desktop Protocol)-account in te loggen. Via RDP is het mogelijk om systemen op afstand te bedienen. Nadat de aanvallers toegang hadden gekregen werden negen werkstations en twee servers met ransomware geïnfecteerd. Op de machines stonden de gegevens van meer dan tienduizend patiënten. Nadat de kliniek de aanval ontdekte was het niet in staat om de getroffen servers via een back-up te herstellen.

Het Office for Civil Rights (OCR) van het Amerikaanse ministerie van Volksgezondheid deed onderzoek naar het datalek en ontdekte dat de kliniek de Health Insurance Portability and Accountability Act (HIPAA) op meerdere punten had overtreden. Deze wetgeving bevat onder andere regels voor zorginstanties voor het beschermen van 'beschermde gezondheidsgegevens'.

Zo had de kliniek geen risicoanalyse uitgevoerd naar de risico's en kwetsbaarheden van beschermde gezondheidsinformatie in de eigen systemen. Ook waren er geen maatregelen getroffen om logbestanden periodiek te controleren en ontbraken beleid en procedures voor het omgaan met beveiligingsincidenten. Naast het betalen van de 500.000 dollar moet de kliniek een beveiligingsplan doorvoeren, waaronder het uitvoeren van risicoanalyses en implementeren van beleid en procedures met betrekking tot gezondheidsgegevens.

Microsoft stelt uitrol van Windows Recall opnieuw uit, nu naar december

Nog geen reacties

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](#) 