

Een cyber nachtmerrie



Over Techni Team

Techni Team is een organisatie met een transparante werkwijze, een proactieve houding, die servicegericht is en meedenkt met de klant. Techni Team beschikt over een ultramodern serverplatform ingericht in een robuust datacenter, waardoor maximale performance kan worden geleverd. **Techni Team is gecertificeerd om 'beveiligde datalijnen' te faciliteren.** Indien gewenst kan zo direct via een beveiligde verbinding connectie met het datacenter gemaakt worden.

Momenteel maken ca. 250 organisaties gebruik van de diensten van Techni Team. **Een groot aantal van deze klanten bevindt zich in de zorg.** Voor deze klantengroep en hun patiënten is databeveiliging en de beschikbaarheid van data een belangrijk thema. Techni Team is dan ook gericht op het beveiligen van data en streeft altijd naar optimale integriteit, beschikbaarheid en vertrouwelijkheid.

Techni Team is qua systemen, medewerkers, processen en procedures volledig ingericht om de klant te ontzorgen en te laten focussen op haar kernactiviteiten.



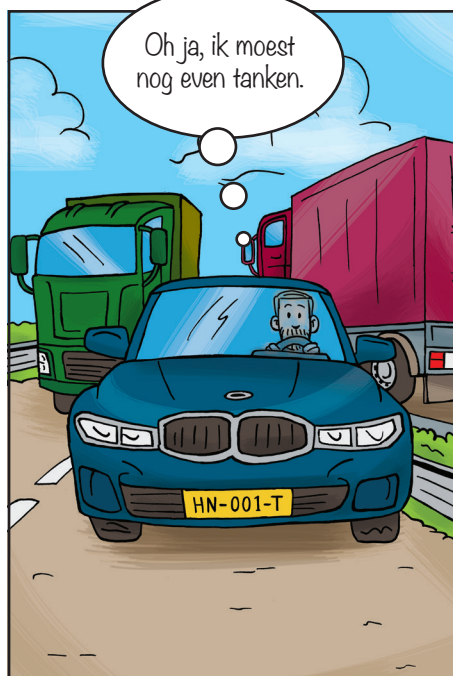
Security Services - Server Hosting - Werkplek Hosting

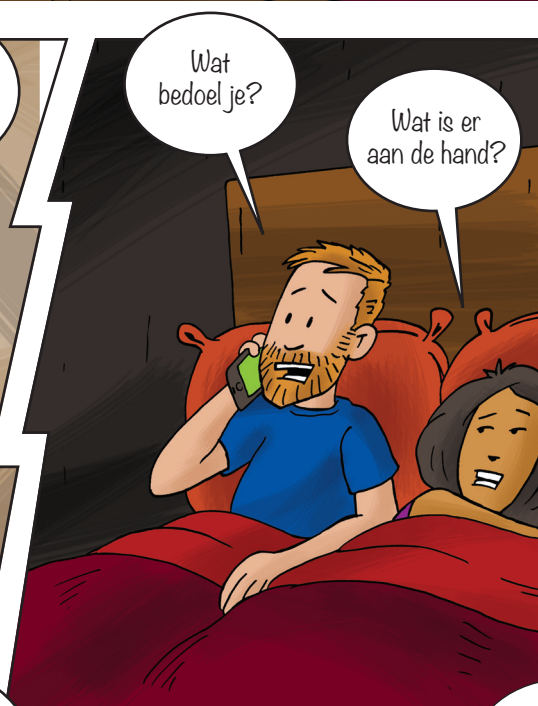
info@techniteam.nl

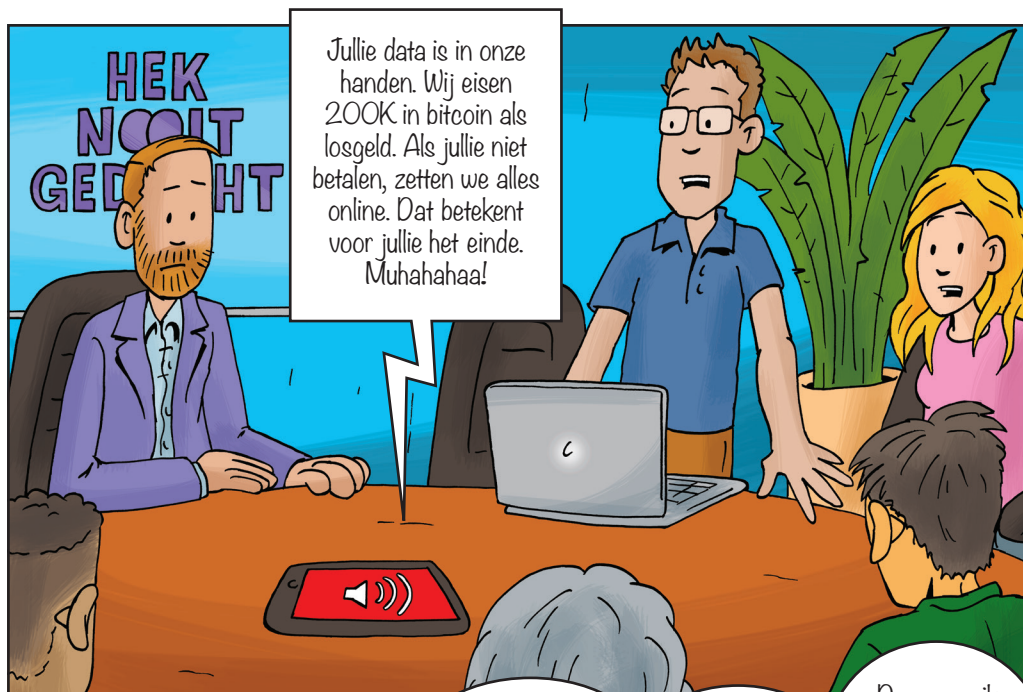
0318 - 57 43 95

Schietboom 2, 3905 TD Veenendaal

www.techniteam.nl



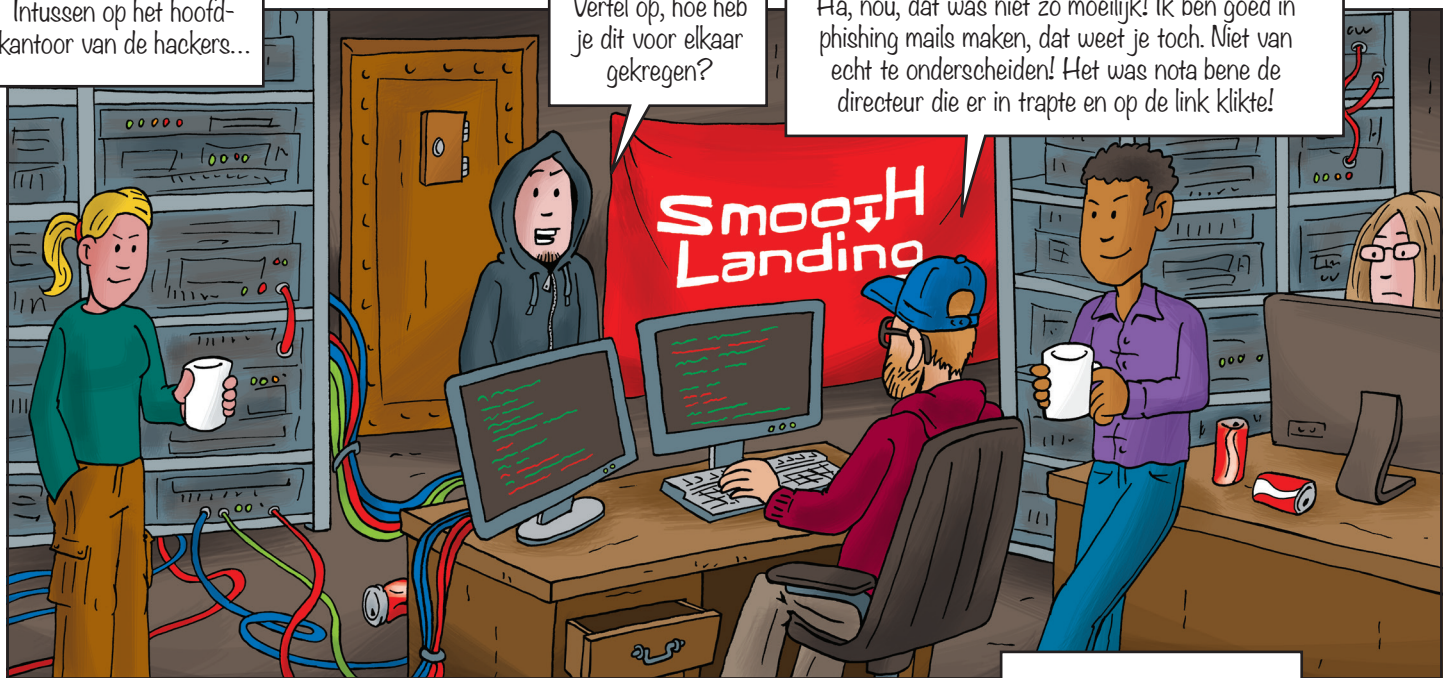




Intussen op het hoofdkantoor van de hackers...

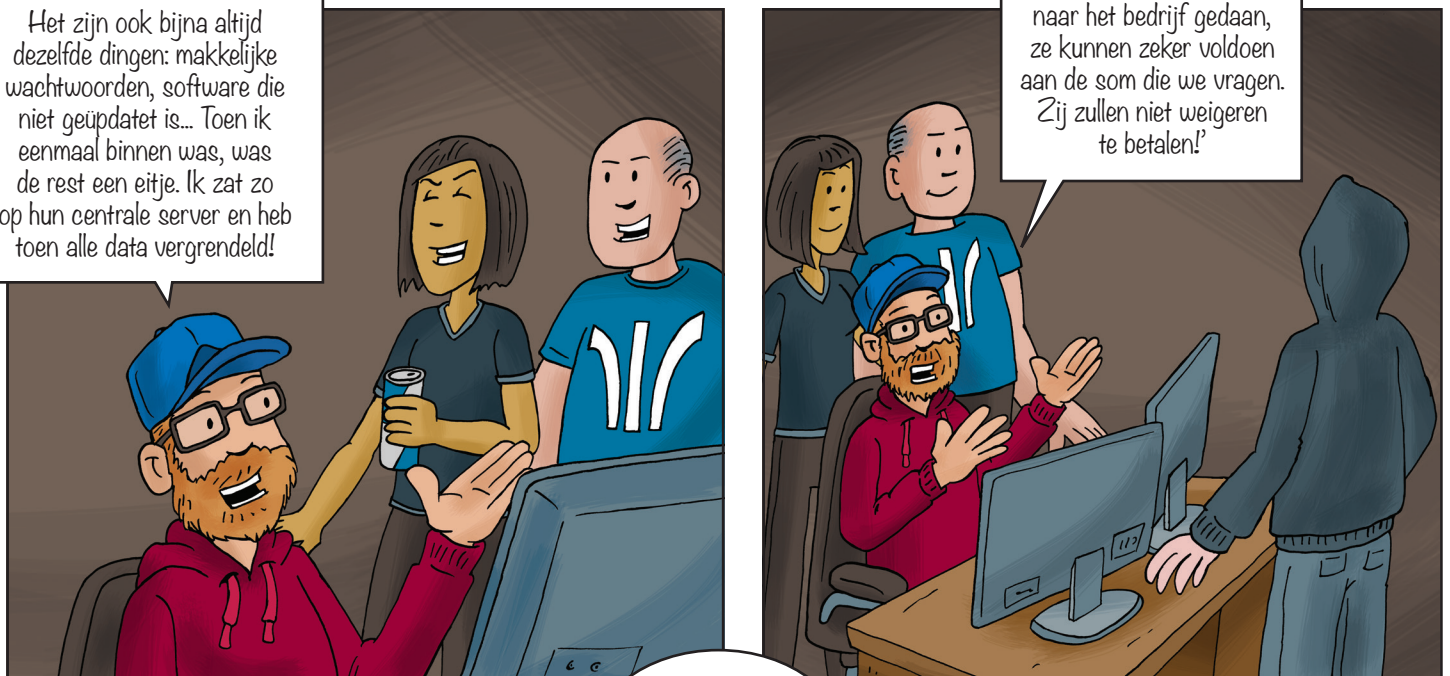
Vertel op, hoe heb je dit voor elkaar gekregen?

Ha, nou, dat was niet zo moeilijk! Ik ben goed in phishing mails maken, dat weet je toch. Niet van echt te onderscheiden! Het was nota bene de directeur die er in trapte en op de link klikte!



Het zijn ook bijna altijd dezelfde dingen: makkelijke wachtwoorden, software die niet geüpdatet is... Toen ik eenmaal binnen was, was de rest een eitje. Ik zat zo op hun centrale server en heb toen alle data vergrendeld!

Ik heb ook wat onderzoek naar het bedrijf gedaan, ze kunnen zeker voldoen aan de som die we vragen. Zij zullen niet weigeren te betalen!'



Die zaterdagochtend op kantoor...

Sjonge, ben je de hele nacht aan het werk geweest?

Zucht, je hebt geen idee.. Ik zit aan m'n achtste bak koffie.



We kunnen nog nergens bij. Ik ben vannacht druk geweest met...

KIJK! Wat moeten we doen?!







En net nu we op het punt stonden om een nieuw huis te kopen. Dat zal wel niet door kunnen gaan.

Zucht, ik zal straks de makelaar wel bellen...

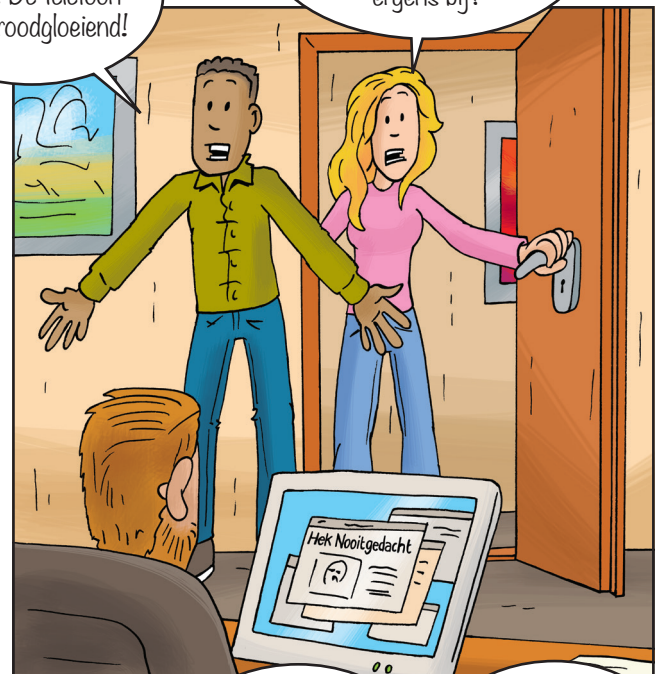
We moeten iets doen! De telefoon staat roodgloeiend!



Ondertussen...

Mijn levenswerk... Straks is alles verloren...

Wat zeggen we tegen de pers? Is er al iets bekend? Kunnen we alweer ergens bij?



Ik vrees dat ik nog meer slecht nieuws heb. Ik kan de back-ups niet terugzetten. We zullen wel moeten betalen, om te redden wat er te redden valt...

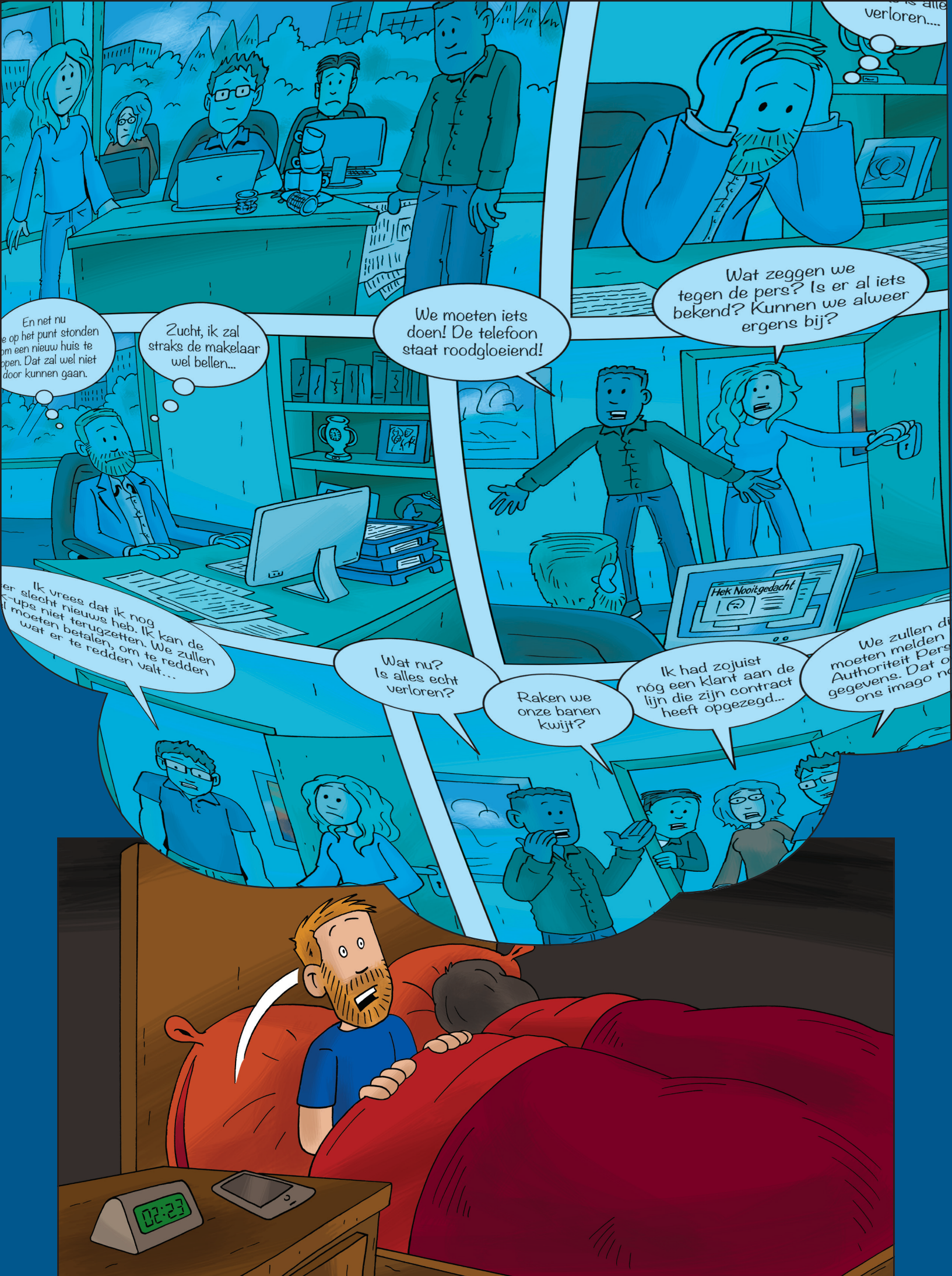
Wat nu? Is alles echt verloren?

Raken we onze banen kwijt?

We zullen dit moeten melden bij de Autoriteit Persoonsgegevens. Dat overleeft ons imago nooit...

Ik had zojuist nog een klant aan de lijn die zijn contract heeft opgezegd...





...is alle
verloren....

En net nu
we op het punt stonden
om een nieuw huis te
kopen. Dat zal wel niet
door kunnen gaan.

Zucht, ik zal
straks de makelaar
wel bellen...

We moeten iets
doen! De telefoon
staat roodgloeiend!

Wat zeggen we
tegen de pers? Is er al iets
bekend? Kunnen we alweer
ergens bij?

Ik vrees dat ik nog
er slecht nieuws heb. Ik kan de
k-lups niet terugzetten. We zullen
moeten betalen, om te redden
wat er te redden valt...

Wat nu?
Is alles echt
verloren?

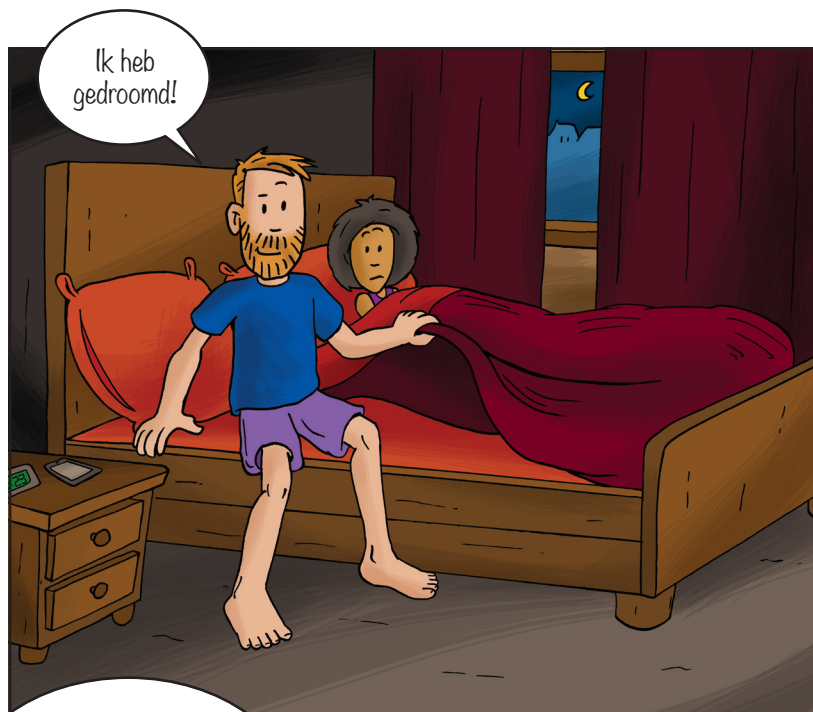
Raken we
onze banen
kwijt?

Ik had zojuist
nog een klant aan de
lijn die zijn contract
heeft opgezegd...

We zullen di
moeten melden
Autoriteit Pers
gegevens. Dat o
ons imago no

Hek Nooitgedacht

02:23



Dat maakt niet uit.
Ik moet direct aan de slag!
Mijn bedrijf loopt gevaar, en
als ik nu niets doe, kunnen
wij straks geen
huis kopen!



Leuke strip, maar dat overkomt mij niet...

Alleen al in 2022 zijn er **21,151 datalekmeldingen** gedaan bij de Autoriteit Persoonsgegevens. De incidenten vinden in elke branche plaats en zowel grote als kleine bedrijven worden slachtoffer van cybercriminelen. Dat betekent helaas dat het ook bij uw bedrijf kan gebeuren.

AP: Boete orthodontiepraktijk vanwege onbeveiligde patiëntenwebsite

10 juni 2021

Thema's: [Beveiliging van persoonsgegevens](#), [Gezondheidsgegevens gebruiken en de \(BSN\)](#)

Ziekenhuisapothek misbruikt voor phishing



Carina van Aartsen 10 oktober 2023, 10:05 895 keer gelezen

Het ziekenhuis ziekenhuis waarschuwt voor nepmails van de ziekenhuisapothek.

3 ov

RTLnieuws

Nieuws Economie Sport Entertainment Tech Lifestyle Editie NL Uitzendingen

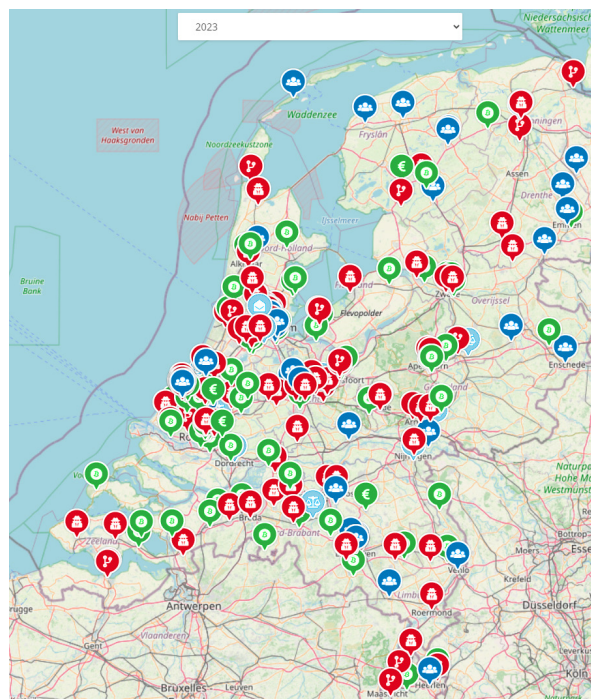
Grote cyberaanval

Tandartsketen betaalt 2 miljoen euro losgeld aan criminelen na cyberaanval

10 augustus 2022 10:19 • Aangepast 10 augustus 2022 17:40

Vroeger zochten cybercriminelen vaak specifieke targets uit, veelal grote bedrijven, waar duidelijk iets te halen is. Tegenwoordig zijn de aanvalsmethodes meer te vergelijken met schieten met hagel. **Elk willekeurig target kan geraakt worden.** Wanneer ze een bedrijf raken, stelen of vergrendelen ze bijvoorbeeld data en eisen losgeld.

Datalekken in Nederland die in 2023 in het nieuws zijn geweest.
Bron: datalekt.nl - januari 2024



Wat zijn de gevolgen van een cyberincident?

Een cyberincident kan veel, vergaande gevolgen hebben. Door gecompromitteerde data ontstaan bijvoorbeeld reputatieschade en vertrouwensverlies. Hierdoor besluiten soms klanten of investeerders om zich terug te trekken. Tijdens een incident kunnen de bedrijfssystemen stilgelegd worden, wat leidt tot omzetverlies. Verder is er financiële schade door losgeld, boetes, schadeclaims, etc. Bij 1 op de 10 bedrijven leidt een cyberincident tot faillissement. Alle reden dus, om je zorgen te maken.

Maar...

Gelukkig is hiermee niet het laatste woord gezegd. Je kunt je verdedigen tegen cybercrimelen en wij vertellen je hoe.

Tips tegen phishing

Een van de meest gebruikte aanvalstechnieken is phishing. Een methode om via e-mails of andere communicatiekanalen te proberen gegevens te ontfutselen of je op een gevaarlijke link te laten klikken. Phishing kan voorkomen worden door kennis en bewustzijn te creëren bij alle mensen binnen een organisatie. Daarmee verbetert de beveiliging significant. Hieronder staan tips om phishing te voorkomen:

Controleer de afzender van een e-mail;

Wees extra alert wanneer de mail een gevoel van **angst, urgentie, autoriteit, vertrouwen of nieuwsgierigheid** opwekt;

Komt de e-mail uit het niets of **verwacht je een dergelijke e-mail?**

Klik nooit zomaar op een linkje of bijlage;

Neem contact op met de afzender om de mail te verifiëren via **de bij jou bekende contactgegevens**, wanneer je het niet vertrouwt.

Geef nooit **vertrouwelijke informatie** door.

10 tips voor sterke databeveiliging

01 Weet wat je hebt

Zorg dat je weet welke IT-middelen (hard- en software) er in je netwerk aanwezig zijn. Je kan niet beschermen waarvan je niet weet dat je het hebt.

02 Multi factor authenticatie

Gebruik zo veel mogelijk multi factor authenticatie. Zorg ook voor sterke wachtwoorden.

03 Update software

Zorg dat je software up-to-date is, om zwakke plekken te voorkomen.

04 Versleutel gegevens

Versleutel bedrijfsinformatie altijd. Ook als je bijvoorbeeld even een USB-stick mee naar huis neemt.

05 Toegangsrechten

Zorg dat medewerkersaccounts alleen toegang hebben tot informatie en systemen die ze echt nodig hebben.

06 Beperk ingangen

Verbind zo min mogelijk apparaten aan het internet.

07 Basismaatregelen

Zorg voor basismaatregelen, zoals een moderne virusscanner en een firewall.

08 Logbestanden

Zorg dat logbestanden op een separate logserver staan. Dan kunnen ze eenvoudiger geanalyseerd worden.

09 Back-up beleid

Zorg voor een goede back-up en test regelmatig of je de back-up ook terug kunt halen. Koppel altijd één back-up los van het netwerk en bewaar die op een andere locatie.

10 Human firewall

Zorg dat medewerkers bekend zijn met de gevaren en risico's. Train medewerkers regelmatig in security awareness.

Wat kan Techni Team voor jou betekenen?

Werkplekhosting bij Techni Team betekent dat alle facetten van uw ICT worden beheerd en verzorgd en **alle ICT-gerelateerde taken uit uw praktijk verdwijnen**. U krijgt nieuwe werkplekken in uw praktijk en de installatie, ondersteuning en het onderhoud daarvan worden u uit handen genomen. Zowel op de voorgrond als achter de schermen, zorgt Techni Team ervoor dat alles optimaal werkt.

Hierbij staat databeveiliging hoog in het vaandel. We hebben bijvoorbeeld een beveiligd datacenter waar al uw vertrouwelijke informatie veilig is. Ook bieden we security awareness trainingen aan, zodat iedereen in het bedrijf leert om veilig te werken.

Investeren is niet nodig, **u betaalt een vast bedrag per maand**. Techni Team investeert, u wordt ontzorgd.

Dit zeggen onze klanten

‘Ik kan niets anders zeggen dan dat ik heel tevreden ben.
Ik zou zo nog een keer met Techni Team in zee gaan.’

Henk van Diermen

Orthodontist Nijkerk

‘Tot nu toe zijn we heel tevreden. Als er eens een keer iets is met hardware of software, wordt dat opgelost.’

Henk Jan Dekens

Huisartsenpraktijk Oldeberkoop

Al jaren besteed ik de ICT uit via Techni team. Dit bevalt prima. Altijd korte wachttijden als je belt bij problemen en problemen worden adequaat opgepakt en verholpen.

Merijn Lambers

Huisartsenpraktijk Lambers