www.ct.nl

c't IT-magazine voor de liefhebber

2022

# SECURITY-CHECKLIST

## Bescherm je netwerk, apparaten, accounts en meer


**Met deze security-checklist ben je in een paar stappen snel beschermd tegen de meeste cyberaanvallen**

# ALLES VEILIG ACHTER SLOT EN GRENDEL

De grens tussen je thuiskantoor en het privéleven wordt steeds minder scherp – en door nieuwe vrijheid om te kiezen op welke plek je hybride gaat werken, is dat voor veel mensen het nieuwe normaal. Het is dus hoog tijd om de beschermingsschilden van de betrokken computers, smartphones, routers, online accounts enzovoort eens goed te controleren en te verbeteren.

Zelfs als je je apparaten alleen voor zakelijke of voor privédoeleinden gebruikt, is een regelmatige controle van de beveiliging aan te raden. Het verandert dagelijks waar de bedreigingen vandaan kunnen komen, en als je daar niet op reageert maak je het online criminelen makkelijker dan nodig is. Daarom willen we je ook dit jaar aanmoedigen om een paar minuten van je tijd te investeren in je IT-security.

We hebben de basisstappen voor de beveiliging van je computer, smartphone, router, accounts en nog veel meer in deze security-checklist samengevoegd. Het duurt maar even om een checklist door te nemen en verbeteringen aan te brengen. Je leert meteen ook hoe je gegevensverlies kunt voorkomen door een trojanbestendige back-up te maken en wat een veilig wachtwoord is. Als je de tips in deze artikelen ter harte neemt, ben je immuun voor de meest voorkomende cyberaanvallen.

De checklist is makkelijk te begrijpen en uit te voeren. Iedereen moet een basisbescherming tegen hackers kunnen instellen. De checklist bevat bewust alleen de belangrijkste stappen die je moet nemen om je te beschermen tegen de meest voorkomende cyberaanvallen. Je kunt de verschillende punten afvinken als je ze gecontroleerd of uitgevoerd hebt.

Gun jezelf dus die paar minuten, loop de verschillende aanvalsmogelijkheden voor hackers even een voor een na en zet een vinkje bij wat je al gedaan hebt.

Veel plezier

Noud van Kruysbergen

PS: een toelichting op deze checklist staat in c't 1-2/2022.

## INHOUD

# Veilig thuis werken

## Security-checklist thuiskantoor

### VEILIGE WERKPLEK

Beveilig je thuiskantoorcomputer altijd volgens de laatste stand. Update het besturingssysteem en de virusscanner regelmatig. Zorg ervoor dat je vanuit je thuiskantoor uitsluitend toegang tot het bedrijfsnetwerk krijgt via een versleutelde VPN-verbinding. Vergeet ook niet om je kantoor of werkplek af te sluiten.

Bescherm de gegevens van je werkgever in je thuiskantoor bijzonder goed: geef niets onzorgvuldig door, verwijder bestanden die je niet nodig hebt en versleutel usb-sticks en harde schijven of ssd's – vooral op laptops. Bescherm de computer met een vergrendelscherm en een wachtwoord.

### GEGEVENS SCHEIDEN

Als je je eigen computer moet gebruiken voor het werk in je thuiskantoor, stel daar dan een apart gebruikersaccount voor in. Bedrijfsgegevens horen niet op een privéaccount te staan. Ga vanuit je werkaccount niet naar persoonlijke clouddiensten als Dropbox en dergelijke.

Om de professionele en privécontacten op je smartphone te scheiden, moet je met extra gebruikersaccounts werken. Als alternatief voor e-mails, contacten en agenda's zijn mobiele Exchange-clients beschikbaar zoals Nine van 9Folders of toegang via webmail.

### VERMIJD VERLIES

Sla belangrijke documenten en gegevens niet op je computer op, maar op de server van het bedrijf. Daar worden automatisch back-ups van gemaakt en dan kun je ook op kantoor meteen verder werken. Als je de bestanden toch lokaal moet opslaan, stel dan in elk geval een automatische synchronisatie in. Vermijd het heen en weer slepen van documenten op usb-sticks.

### VIDEOCHATTEN

In het thuiskantoor staan je gesprekspartners eigenlijk nooit tegenover je – gunstige omstandigheden voor cybercriminelen. Videochat-deelnemers zonder een camera kunnen collega's maar ook aanvallers zijn.

E-mails van je baas kunnen echt zijn, maar ook een poging tot phishing. Mocht je twijfelen, bel dan even na.

### CONTACT MET DE BASIS

Niet alles werkt meteen, soms ontbreekt er iets om door te werken, soms loopt het VPN vast, soms gaat de computer kapot. De snelste oplossing is niet altijd de veiligste. Blijf daarom in contact met de beheerders van je bedrijf en maak een lijst van de belangrijke contactpersonen voor noodgevallen.

# Alle ramen goed op slot

## Security-checklist Windows

### UPDATES INSTALLEREN

Microsoft biedt regelmatig updates voor beveiligingslekken in Windows. Een controle zou niet meer dan een paar dagen geleden moeten zijn. Laat Windows daarbij ook andere Microsoft-programma's zoals Office up-to-date houden.

Microsoft voorziet oude versies van Windows niet meer van beveiligingspatches, je moet ten minste Windows 8.1 gebruiken. Voor Windows moet je belangrijke functie-upgrades binnen 18 maanden installeren. Houd ook de geïnstalleerde applicaties up-to-date.

### CONTROLEER JE ANTIVIRUS

Een antivirusprogramma kan je helaas niet tegen alle bedreigingen beschermen. Bij Windows is Windows Defender standaard geïnstalleerd. Zorg ervoor dat hij actief is en voorzien is van de laatste virushandtekeningen.

### ACTIVEER DE TOEGANGSBEVEILIGING

Je computer moet ook worden beschermd tegen fysieke toegang. Het beste kun je de harde schijf of ssd versleutelen met BitLocker of, bij Windows Home, met VeraCrypt. Dan zijn je gegevens beschermd, zelfs als iemand direct toegang tot de gegevensdrager heeft.

Beveilig je Windows-gebruikersaccount met een wachtwoord van ten minste 10 tekens. Vergrendel je computer als je aan de wandel gaat. Dat kan snel en eenvoudig met de toetsencombinatie Windows+L. Je kunt ook instellen dat Windows automatisch wordt vergrendeld als je het niet gebruikt, voor het geval je dat vergeet.

### VERBETER DE GEGEVENSBESCHERMING

Zorg ervoor dat er niet meer gegevens naar Microsoft worden verzonden dan nodig is. Zoek in het Startmenu naar 'Diagnostische gegevens en feedback' en zorg ervoor dat 'Vereiste diagnostische gegevens' onder 'Diagnostische gegevens' geselecteerd is.

Windows heeft het liefst dat je een Microsoft-account gebruikt, maar gebruik als dat kan een lokaal account. Bij Windows 11 Home is dat helaas niet meer mogelijk.

### DATADIEFSTAL VOORKOMEN

Je gegevens zijn op een systeemschijf omdat die kan crashen. Je loopt daarbij ook het risico dat de bestanden door een crypto-trojan worden versleuteld.

Maak daarom back-ups van alle belangrijke gegevens door ze bijvoorbeeld naar een usb-stick te kopiëren.

# Veilig mobiel

## Security-checklist smartphone

### FIRMWARE-UPDATES

Of je nu Android of iOS als besturingssysteem gebruikt, zorg ervoor dat je altijd de meest actuele versie hebt.

Apple voorziet zijn iPhones op voorbeeldige wijze van updates. Bij Android is de situatie nogal wisselend, vooral bij de goedkopere smartphones droogt de stroom aan updates vaak na een korte tijd al op. Je kunt bij de instellingen altijd controleren of er een update is. Daar kun je het installeren ook meteen in gang zetten.

Als je een smartphone gebruikt waar de fabrikant verder niet meer naar om lijkt te kijken, moet je een nieuwe aankoop overwegen.

### ACTIVEER DE TOEGANGSBEVEILIGING

Zorg ervoor dat het vergrendelscherm ingesteld is en dat er een wachtwoord gedefinieerd is om te ontgrendelen. Het wachtwoord moet niet te makkelijk te raden zijn: 1234, 5555 of je geboortedatum zijn taboe.

Gebruik bij voorkeur een wat langer wachtwoord, de meeste smartphones kunnen meestal toch eenvoudig worden ontgrendeld door middel van een gezichtsscan of vingerafdruk. Het wachtwoord dient dan alleen als back-up en hoeft zelden te worden ingevoerd.

### VERMIJD EXTERNE BRONNEN

Installeer alleen apps uit de officiële app-stores. Die worden in ieder geval aan een veiligheidscontrole onderworpen. Als je bij Android een app als APK-installatiepakket wilt installeren, moet je die rechtstreeks bij de ontwikkelaar halen. Zorg er dan voor dat Play Protect actief is.

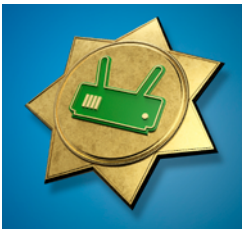
### APP-MACHTIGINGEN

Voordat je een app installeert, moet je controleren welke machtigingen er precies nodig zijn. iOS-gebruikers kunnen de reeds verleende rechten beheren onder ‘Instellingen / Privacy’, Bij Android kun je kijken bij het applicatiebeheer.

### NIET JAILBREAKEN

Het is mogelijk om een smartphone te rooten (Android) of jailbreaken (iOS) om hogere rechten op je apparaat te krijgen en ingrijpende wijzigingen in het systeem aan te brengen. Dat zorgt echter ook voor het omzeilen van essentiële beveiligingsfuncties, waardoor hem eigenlijk beter in zijn oorspronkelijke toestand kunt laten.

Bovendien weigeren veel apps op een dergelijke aangepaste smartphone gelukkig om te starten vanwege veiligheidsproblemen.



# Netwerk beveiligen

## Security-checklist wifirouter

### WEBINTERFACE BEVEILIGEN

Bijna elke router heeft een wizard die je vraagt om enkele van de belangrijkste instellingen en die dan in één keer configureert. De wizards laten afhankelijk van de fabrikant daarbij echter verschillende gaten in het systeem zitten.

Zorg er voor dat het door de fabrikant zelf ingestelde configuratiewachtwoord gewijzigd is. Wie de toegangsgegevens van je router weet, kan met je router doen wat hij wil.

Activeer indien aanwezig een automatische firmware-update.

### WIFI-MAATREGELEN

Schakel de beveiliging van controlepakketten (PMF) in als dat kan. Wijzig de naam van het draadloze netwerk en de sleutel ervan (het wifiwachtwoord).

Bij routers die alleen de oudere WPA2-standaard gebruiken, kan de encryptie worden gekraakt door een brute-force-attack. De lengte van je wifiwachtwoord bepaalt of het kraakproces snel succesvol kan zijn of dat het na een paar dagen wordt opgegeven omdat het uitzichtloos lijkt te worden.

Gebruik 20 tot 30 tekens voor het wachtwoord als je WPA2 in je wifinetwerk moet gebruiken. Als al je apparaten WPA3 al ondersteunen, schakel WPA2 dan uit als dat kan.

### GEBRUIK HET GASTNETWERK

Scherm je vertrouwde apparaten af van de apparaten die bezoekers bij zich hebben en ook van smarthome- en IoT-apparaten door het gastwifi daarvoor te gebruiken. Beperk het gastnetwerk tot bepaalde diensten, zoals surfen en e-mailen, om ongewenste bestandsuitwisseling te voorkomen.

### NIET ZONDER TLS

Als je een server gebruikt die toegankelijk is vanaf internet, zorg er dan voor dat die alleen communiceert via met TLS versleutelde protocollen.

Aangezien sommige routers ook een webinterface hebben die vanaf internet toegankelijk is, moet het bijbehorende verkeer dan ook worden versleuteld (HTTPS).

### WPS ALLEEN INDIEN NODIG

Activeer WPS alleen wanneer dat nodig is. Anders kunnen derden buiten jouw medeweten om toegang krijgen tot je netwerk als ze bij de router kunnen.

Schakel UPnP indien mogelijk ook uit of beperk het tot individuele hosts als je router dat toelaat.

Exporteer de routerconfiguratie, zodat je met een vervangend exemplaar meteen verder kunt.

# Brief-geheimen

## Security-checklist e-mail

### GEZOND WANTROUWEN

E-mails zijn niet veilig, dat is inmiddels algemeen bekend. Goed uitgevoerde vervalsingen kunnen op dit moment grotendeels automatisch worden aangemaakt. Wantrouw dus in principe elke e-mail en wees vooral alert als er links, bijlagen of geld in het spel zijn.

### BEVEILIGING VAN JE MAILCLIENT

Je moet in het algemeen het laden van externe inhoud verbieden. Die externe content wordt namelijk vaak gebruikt voor (reclame)tracking en is altijd betrokken bij beveiligingslekken.

Schakel de HTML-weergave uit of stel je client in elk geval in om de voorkeur te geven aan pure tekstinhoud. Bij veel mailclients kun je dat direct vanuit de mailweergave doen, zodat het verlies aan comfort minimaal is.

Je moet er ook voor zorgen dat bij de instellingen van je e-mailcliënt de mails alleen via STARTTLS of TLS/SSL worden opgehaald en verzonden.

### ENCRYPTIE

E-mails zijn eigenlijk vergelijkbaar met ansichtkaarten: iedereen die ze onderweg in handen krijgt kan ze lezen. Veel providers ondersteunen tweefactor-authenticatie (2FA), dat maakt het een stuk lastiger om je account te compromitteren.

Het is gebruikelijk dat e-mails versleuteld worden verstuurd. Dan kan de ‘postbode’ ze nog wel lezen, maar niet iedereen die toegang heeft tot de datastroom. End-to-end-versleuteling is voor e-mails ook mogelijk, met behulp van S/MIME of OpenPGP. Veel mailclients ondersteunen beide methoden, maar de tussenliggende dienst moet ook meewerken. Als noodoplossing bieden sommige providers aan om e-mails automatisch te versleutelen bij ontvangst via OpenPGP of S/MIME.

### VERSTANDIG GEBRUIK

Door het versturen van gewone tekstberichten kun je geen fancy opmaak toepassen, maar het wel is veel veiliger.

Verstuur in principe geen uitvoerbare bestanden of Office-documenten met macro’s erin.

Je moet ook goed kijken naar de lijst van ontvangers: de optie ‘Allen beantwoorden’ is dan wel handig, maar vaak teveel van het goede en de optie verspreidt de informatie verder dan nodig is. Controleer verder voor het verzenden of de gehele originele mail echt moet worden geciteerd – vooral als je de ontvangerskring groter maakt. Vaak kun je wat meer gevoelige informatie beter via een telefoongesprek doorgeven.

# Whats-Secure?

## Security-checklist messengers

### VERSLEUTELING GEBRUIKEN

WhatsApp en Signal versleutelen alles in principe altijd end-to-end. Apps zoals Telegram en Facebook Messenger zijn geschikt voor E2EE, maar gebruiken dat normaal gesproken niet. Bij die apps moet je erop letten dat je een afzonderlijk 'geheim' gesprek of chat start.

E2EE-codering in de vorm van een double-ratchet-procedure is beschikbaar voor XMPP-clients via het OMEMO-protocol, dat al door een heleboel clients ondersteund wordt.

Zoom werd in het begin afgeraden omdat de verbindingen niet versleuteld werden. Op de server werden de verbindingen inderdaad ontsleuteld om ze daarna versleuteld weer naar meerdere gebruikers tegelijk te kunnen sturen. Dat werd gelukkig snel aangepast, waardoor het populaire Zoom verder veilig gebruikt kan worden.

### WIE LUISTERT MEE?

Veel messengers bieden naast de app ook web- of desktopclients. Als je een web- of desktopclient open hebt staan, zijn alle gesprekken echter zonder meer mee te lezen. De messenger-apps op de smartphone laten daarom zien welke andere apparaten ermee gekoppeld zijn. Controleer die lijst regelmatig en verwijder wat je niet meer nodig hebt.

### BACK-UPS CONTROLEREN

Sommige apps zoals WhatsApp en Signal maken automatisch of op verzoek versleutelde back-ups aan. Dat helpt niet als de telefoon kapot gaat – je moet dergelijke back-ups regelmatig op een ander apparaat zetten. Wees sceptisch tegenover back-ups naar de cloud.

Bij sommige messengers kun je berichten automatisch laten verwijderen na een bepaalde tijd. Dat verhindert echter niet dat de gesprekspartner die berichten bewaart.

### VERIFICATIE ACTIVEREN

Veel messengers koppelen de accounts aan een mobiel telefoonnummer. Veel messengers bieden aan om het registratieproces te beveiligen met een extra pincode. Die functie moet je gebruiken, maar bewaar de pincode goed.

### EERST NADENKEN, DAN KLIKKEN

Ook bij messengers lopen er criminelen rond die kettingbrieven en ongevraagde reclame rondsturen. Voeg dan ook niets en niemand aan je contacten toe zonder dat eerst goed te controleren.

Zet geen privégegevens in je (openbare) accountprofiel. En besef dat geen enkele beveiliging een vervanger is voor gezond wantrouwen.

# Veilig surfen op internet

## Security-checklist browsers

### UP-TO-DATE BLIJVEN

Om veilig op internet te kunnen surfen, moet je altijd de laatste versie van je browser gebruiken. De makers brengen voortdurend updates uit die veiligheidsgaten dichten. Google elimineert per maand soms tot wel vijftien kwetsbaarheden met een Chrome-update.

In het ideale geval werkt je browser zichzelf automatisch bij en wordt Microsoft Edge door Windows up-to-date gehouden. Af en toe blijft zo'n update echter hangen of moet de browser opnieuw worden opgestart.

### ADD-ONS UITMESTEN

Browseruitbreidingen hebben toegang tot alles wat er in je browser gebeurt. Zorg ervoor dat je precies controleert waar je aan begint voordat je er een installeert. Installeer alleen uitbreidingen uit de officiële downloadcatalogi van de producent en let op de downloadaantallen en gebruikersbeoordelingen. In geval van twijfel is het in het belang van de veiligheid van je browser beter om het zonder add-ons te doen. Controleer ook welke uitbreidingen al geïnstalleerd zijn en mest de boel eens grondig uit. Bij Chrome staan ze in het menu onder 'Meer hulpprogramma's', bij Firefox klik je op 'Add-ons'. In het Edge-menu klik je op Extensies.

### BLOKKEER TRACKERS

Blokkeer alle trackers die bijhouden waar je op internet bent geweest. Je hoeft bij Edge de tracker-blocker alleen in te schakelen bij de instellingen onder 'Privacy, zoeken en services'. Voor andere browsers bestaan add-ons als Privacy Badger en uMatrix.

### MACHTIGINGEN CONTROLEREN

Websites kunnen om toestemming vragen voor toegang tot je camera, microfoon en locatie. Controleer de reeds verleende toestemmingen regelmatig en ruim ze grondig op.

### LET OP URL'S

Geef persoonlijke informatie of wachtwoorden alleen op websites die in versleutelde vorm worden verzonden – de url begint dan met https:// of je browser toont een (groen) gesloten hangslot naast het adres.

Bovendien moet je de webadressen zorgvuldig controleren op inconsistenties. Een verkeerde letter of een vreemd karakter is voldoende om je niet naar je bank door te sturen, maar naar een perfect gekopieerde phishing-site. Het is het beste om regelmatig bezochte websites te bookmarken en in het vervolg ze van daaruit te bezoeken.

# Sociale zekerheid

## Security-checklist sociale media

### GEBRUIK TWEE FACTOREN

Als je socialemedia-accounts worden gehackt, kunnen de gevolgen rampzalig zijn. Niet alleen voor jou, maar ook voor je vrienden en zakenpartners. Maak gebruik van alle mogelijkheden die de betreffende platforms bieden. Waar mogelijk moet je naast het wachtwoord nog andere toegangsbarrières instellen zoals tweefactor-authenticatie (2FA).

Bij Facebook ga je met 'Instellingen en privacy' en 'Instellingen / Beveiliging en aanmelding' naar de instelmogelijkheden van de tweestapsverificatie. Vergelijkbare instellingen zijn beschikbaar bij alle grote sociale netwerken.

Om te voorkomen dat die vraag telkens opnieuw wordt gesteld, onthouden de platforms apparaat-ID's of stellen ze cookies in en blijven ze ingelogd op het apparaat. Dat kan een beveiligingsprobleem worden als meerdere mensen een computer delen. Controleer van tijd tot tijd welke apparaten op dat moment geautoriseerde toegang hebben tot het account en daarom uitgezonderd zijn van de 2FA.

### TOEGANG CONTROLEREN

Bij veel sociale netwerken kun je externe diensten toegang geven tot je account, bijvoorbeeld voor single-sign-on aanmeldingen op gekoppelde websites. Hou wel een oogje in het zeil op de activiteiten en rechten van die apps.

Instagram vermeldt de actieve apps bij de profielinstellingen. Ruim dat af en toe op. Bij Twitter kun je ook geautoriseerde apparaten verwijderen die geen toegang meer zouden moeten hebben.

### GERICHT DELEN

Je kunt vaak aangeven met wie je content wilt delen. Houd je doelgroep in de gaten, zodat je niet per ongeluk een grotere kring van geadresseerden aanspreekt dan je wilt. Je moet bijvoorbeeld niet in het openbaar posten dat je twee weken op vakantie bent en je huis dus leegstaat. Daarbij moet de standaardinstelling defensief zijn.

### AANVRAGEN CONTROLEREN

Soms zitten er achter vriendschapsverzoeken alleen pogingen om toegang te krijgen tot persoonlijke gegevens. Controleer elke aanvraag zorgvuldig. Nep-accounts hebben vaak profielfoto's van aantrekkelijke mensen.

### PRIVÉBERICHTEN

Wees voorzichtig als iemand een privébericht stuurt en het dringend lijkt – zeker als het over geld gaat. Misschien is het betreffende account gehackt.

# Geld in de online kluis

## Security-checklist online bankieren

### TRANSACTIES CONTROLEREN

Voor bijna alle overschrijvingen is een tweefactor-authenticatie vereist. Controleer bij online overboekingen het IBAN-nummer van de ontvanger. En kijk ook of het bedrag klopt voordat je een overboeking goedkeurt. Vergelijk het IBAN-nummer en het bedrag altijd ook met de gegevens op de factuur. En zoals overal, kies sterke wachtwoorden of pincodes!

### BANKIEREN ZONDER VIRUSSEN

Bankieren met een pc of smartphone is alleen veilig als het systeem vrij is van malware. Zorg ervoor dat op een Windows-pc een virusscanner met de nieuwste updates draait.

### PHISHING HERKENNEN

In de overgrote meerderheid van de gevallen van fraude bij online bankieren, verzenden criminelen gemanipuleerde e-mails of maken ze fake-websites. Daarmee willen ze bepaalde handelingen bij nietsvermoedende gebruikers uitlokken door bijvoorbeeld e-mails namens bankinstellingen. Ze gebruiken die om trojans en andere malware binnen te smokkelen, te linken naar websites met kwaadaardige code of toegang te krijgen tot gegevens (phishing).

Controleer bij alle andere links eerst waar de url naartoe gaat. Let op de taal, veel buitenlandse phishing-mail heeft moeite met de juiste zinsbouw en correcte spelling. Voer je toegangsgegevens pas in de browser in op de website van de bank, en alleen als je het adres zelf hebt getypt.

### CONTROLEER AFSCHRIJVINGEN

Als creditcardgebruiker moet je elk afschrift controleren en eventuele ongeoorloofde afboekingen dan onmiddellijk melden. Controleer ook regelmatig je bankafschriften.

### ROOT JE SMARTPHONE NIET

Root of jailbreak de smartphone of de tablet die je gebruikt voor internetbankieren niet, want dat zal belangrijke beschermende functies lamleggen. Dat is vooral gevaarlijk als je een beveiligingsapplicatie op hetzelfde apparaat gebruikt voor de tweede factor. Gebruik een smartphone met een besturingssysteem dat nog steeds updates krijgt.

Het is aan te raden om in elk geval de richtlijnen van je bank te volgen. Zolang de app van je bank een ouder besturingssysteem nog ondersteunt en je die nog steeds kunt gebruiken, kun je in elk geval niet verweten worden dat je wat dat betreft nalatig gehandeld hebt.

# Veilig back-uppen

## Security-checklist back-ups

### BACK-UP NU!

Elke back-up is beter dan helemaal geen, het belangrijkste is dat je dat ook daadwerkelijk doet – en wel nu!

Begin met de unieke bestanden. Denk ook aan originele foto's, video's en correspondentie. Overweeg voor de rest hoe tijdrovend het is om er opnieuw aan te komen of ze te bewerken.

### VUURBESTENDIG

Als er brand in je huis uitbreekt, zal ook een usb-schijf naast de pc verbranden. Ook een kelder en zolder voldoen niet want het bluswater loopt de kelder in en het vuur gaat overal naartoe. Kortom: de back-up moet het huis verlaten.

### BESCHERMING TEGEN 'OEPS!'

Bestandsverlies ten gevolge van bedieningsfouten en hardware-uitval is niet altijd te voorkomen. Voor kleine hoeveelheden bestanden is een usb-stick of dvd voldoende als opslagmedium.

Sommige bestanden kun je ook op papier afdrukken.

### VEILIG TEGEN TROJANS

Trojans vallen zo'n beetje alles aan waar ze bij kunnen. Daarom is een back-up alleen betrouwbaar als je die technisch gescheiden houdt van het origineel. Hij mag vanaf de broncomputer op geen enkele (!) manier bereikbaar zijn.

Een usb-stick die wordt losgekoppeld is technisch gezien wel gescheiden, maar als je hem weer aansluit is hij dat niet meer. Gebruik daarom meerdere back-upmedia.

### DIEFSTALBESTENDIG

Het is het beste om de back-upmedia in een brandwerende kluis te stoppen. Als alternatief helpt om de back-upbestanden te versleutelen. Verlies de sleutel zelf natuurlijk niet.

### HERSTELLEN

Je moet een back-up als test wel een keer herstellen. Gebruik daar dan een andere pc voor.

### BLIJVEN HERHALEN

Back-ups verouderen, maak dus regelmatig een nieuwe. Of automatiseer dat.

### RUSTIG SLAPEN

Voldoet je back-up aan alle eisen? Gefeliciteerd! Kijk dan eens of je met het programma Duplicati voor jezelf wellicht makkelijk een centrale back-upprocedure kunt instellen.


# Zonder wachtwoord

## Security-checklist wachtwoorden

### NIET RECYCLEN

Gebruik voor elke dienst in elk geval een ander wachtwoord – vooral bij diensten waarbij persoonlijke informatie of geld betrokken is.

### LIEVER LANG

Je hoeft wachtwoorden niet regelmatig te wisselen, je moet ze alleen wijzigen als een account gehackt is of een wachtwoord in verkeerde handen is gevallen.

Een goed wachtwoord moet geschikt zijn voor dagelijks gebruik en moet ook op een smartphone kunnen worden ingetoetst. In plaats van veel speciale tekens kun je beter lange wachtwoorden gebruiken. Vooral bij het versleutelen moet je zo veel mogelijk tekens gebruiken als je kunt verwerken, bijvoorbeeld door woorden aan elkaar te rijgen – spelfouten zorgen voor meer veiligheid.

### WACHTWOORDMANAGER

Al die wachtwoorden voor al die verschillende diensten: je kunt dan beter een wachtwoordmanager gebruiken voor je toegangsgegevens. Die slaan je wachtwoorden veilig versleuteld op computers, smartphones en tablets op. Het enige wat je hoeft te doen, is het hoofdwachtwoord te onthouden om de wachtwoordmanager te ontgrendelen.

Wachtwoorden opslaan in een browser is niet aan te bevelen. Iedereen die toegang heeft tot je account kan dan bij alle opgeslagen gegevens. Als het kan, moet je bij de browser een hoofdwachtwoord instellen.

### BACK-UP OP PAPIER

Als je niet prettig vindt om een wachtwoordmanager te gebruiken, kun je je wachtwoorden natuurlijk ook simpelweg opschrijven met pen en papier. Dat is zelfs trojan-bestendig. Zorg ervoor dat de wachtwoorden niet aan een gebruikersnaam of dienst kunnen worden gekoppeld. Schrijf ze in aangepaste vorm op, gebruik bijvoorbeeld wachtwoorden die altijd beginnen met hetzelfde, bijvoorbeeld ‘ikleesct’, maar schrijf dat dan niet op.

### GEBRUIK TWEE FACTOREN

Tweefactor-authenticatie (2FA) beschermt tegen hackers. Als dat actief is, vraagt de service bij het inloggen niet alleen om het wachtwoord, maar ook om een tweede factor. Een authenticator-app zoals Google Authenticator is nog veiliger. Als alternatief kun je ook een beveiligingssleutel (FIDO2 of U2F) als tweede factor gebruiken. Die hebben meestal het formaat van een usb-stick.

# Vindbaar op internet

## Security-checklist server en hosting

### GEBRUIK TWEEDE FACTOR

Gebruik een tweede factor voor de beheerinterface. Iemand die daar toegang toe krijgt, kan veel schade veroorzaken. Als hij je contactgegevens heeft gewijzigd, moet jij eerst nog bewijzen dat je zelf de rechtmatige eigenaar bent.

### DATALEKKEN DICHTEN

Aanvallers zoeken specifiek naar verouderde versies van servers en scripttalen als die bekende hiaten bevatten. Het is eenvoudig dat te achterhalen via de HTTP-header. Je kunt dat bij Nginx en Apache beperken in het configuratiebestand. Voor de scripttaal PHP kun je dat stoppen met `expose_php = Off` in php.ini. Om te zien of de maatregelen succesvol waren, open je de ontwikkeltools van de browser (meestal met F11) en kijk je naar de netwerkrequest en de antwoorden van de server.

### SSH, MAAR VEILIG

SSH biedt een relatief veilige verbinding naar je server. Het is voor Linux-beheerders al lang de standaard en recentelijk zelfs beschikbaar geworden voor Windows. Om de veiligheid te verhogen, dien je in te loggen met behulp van een public-key en moet je de toegang via wachtwoorden helemaal uitschakelen.

Het wordt vaak aanbevolen om de SSH-server op een andere poort dan 22 te laten werken, maar aanvallers zullen je SSH-server op elke andere poort binnen korte tijd kunnen vinden.

### BLIJF UP-TO-DATE

Houd je systemen up-to-date. Dat geldt voor het besturingssysteem, de webserver en de scripttaal (zoals PHP). Bij webhosters is dat niet zo eenvoudig.

Je moet dan niet alleen naar de logbestanden kijken als er een probleem is, maar dat regelmatig even doen. Controleer ook de logs van de SSH-server of die van Remote Desktop bij Windows regelmatig op afwijkingen.

### VERWACHT BEZOEKERS

Een server die toegankelijk is via het IPv4-adres is niet geheim te houden door er geen domeinnaam voor in te stellen. Beveilig vertrouwelijke informatie daarom altijd met een wachtwoord en activeer HTTPS.

### WACHTWOORDEN HASHEN

Als je een eigen dienst ontwikkelt, sla de wachtwoorden van je gebruikers dan op met een hashmethode zoals PBKDF2 en sla alleen de (bij voorkeur salted) hashwaarde op.

# Voor wie op zoek is naar diepgang en betrouwbare informatie

**Met een c't abonnement krijg je:**

• Uitgebreide onafhankelijke tests, diepgaande achtergronden en workshops op niveau

• Verrassende onderwerpen om je kennis te verbreden

• Toegang tot de digitale versies en pdf's om te archiveren


Ontvang 3x c't magazine voor **€20,-**

## Abonneer je nu via www.ct.nl/abo

of bel naar +31 (0)24 2027 825

Kijk voor de meest actuele prijzen op www.ct.nl/abo. Je abonneert tot wederopzegging en voor ten minste de actieperiode van 10 nummers. Na afloop van de actieperiode geldt de reguliere abonnementsprijs en is het abonnement per kwartaal opzegbaar. Opzeggen is heel eenvoudig en kan via onze klantenservice.

# COLOFON


## C'T IS EEN UITGAVE VAN F&L MEDIA COMPUTER BV

in licentie van
Heise Medien GmbH & Co. KG, Hannover

## ALGEMEEN DIRECTEUR

Arjan Kropman

## BRAND MANAGER

Noud van Kruysbergen

## REDACTIE

Daniel Dupré, Nick Muijs, Marco den Teuling, Alieke van Sommeren

## MET MEDEWERKING VAN

Jo Bager, Holger Bleich, Ronald Eikenberg, Jan Mahn, Markus Montz, Andrea Trinkwalder, Sylvester Trommel, Axel Vahldiek, Dušan Živadinović

## VORMGEVING

Susan Gerbrands, Tom Gerrits, Nick Groenewold, Mylene Nales, Ellen Willemsen

## SALES

Thijs de Hoogh
+31 (0)24 2404641
tdhoogh@fnl.nl

## NIEUWSREDACTIE / PERS

redactie@ct.nl of adresgegevens zie hieronder o.v.v. redactie c't magazine

## BEZOEKADRES F&L MEDIA

Jonkerbosplein 52,
6534 AB Nijmegen