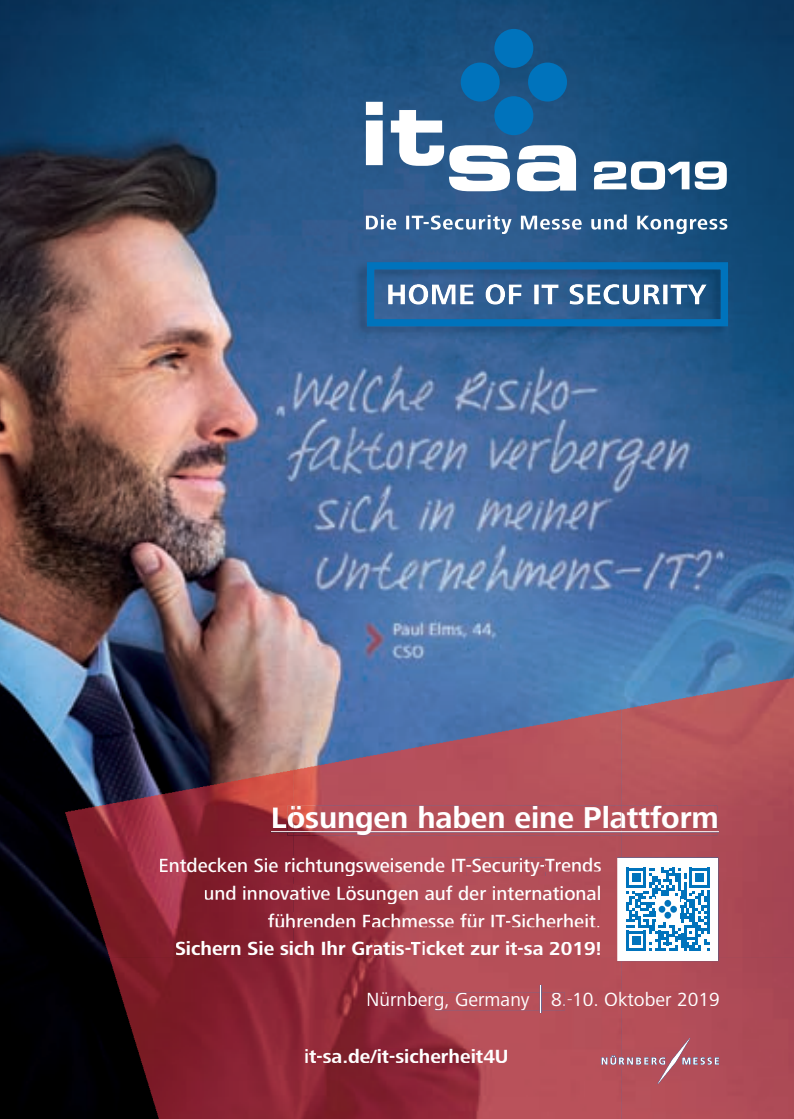
Kompakt

Auflage 2020
Schutz vor aktuellen Gefahren

Sicherheits-Checklisten

Rundumschutz in 5 Minuten

Windows | Android | iOS | Mail | Browser | Online-Banking
WhatsApp | Social Media | WLAN-Router | Raspberry Pi
Backup-Strategien | Sichere Passwörter



it sa 2019

Die IT-Security Messe und Kongress

HOME OF IT SECURITY

Lösungen haben eine Plattform

Entdecken Sie richtungsweisende IT-Security-Trends und innovative Lösungen auf der international führenden Fachmesse für IT-Sicherheit.
Sichern Sie sich Ihr Gratis-Ticket zur it-sa 2019!

Nürnberg, Germany | 8.-10. Oktober 2019

it-sa.de/it-sicherheit4U

NÜRNBERG MESSE

Liebe Leserinnen und Leser,

dieses kleine Heft hat es in sich: Es kann Sie vor dem nächsten Hacker-Angriff beschützen. Sichern Sie Ihre Rechner, Smartphones, Router & Co. durch wenige Handgriffe ab, die jeder versteht. Auch Ihre Online-Accounts schützen Sie mit unseren Checklisten ohne Mühe. Und vor Datenverlusten durch defekte Festplatten oder Erpressungs-Trojaner müssen Sie sich auch nicht mehr fürchten. Wie das alles in so ein kleines Booklet passt? Ganz einfach: IT-Sicherheit ist zwar beliebig komplex, vor den meisten Gefahren können Sie sich jedoch mit wenigen Schritten schützen. Geben Sie das Booklet gern auch an Freunde, Verwandte und Kollegen weiter! Falls Sie sich nicht davon trennen mögen, können Sie dieses kleine Heftchen unter **ct.de/check2020** separat nachbestellen oder gratis als PDF herunterladen.

Inhalt

Und jetzt frisch ans Werk!

Ronald Eikenberg

Windows 10

So viel Schutz muss sein

Windows updaten

Installieren Sie alle verfügbaren Updates, indem Sie „Updates“ ins Startmenü eintippen und auf „Nach Updates suchen“ klicken.

Virenschutz checken

Stellen Sie sicher, dass ein Virenschutz mit aktuellen Virensignaturen installiert ist. Der vorinstallierte Defender reicht aus. Seinen aktuellen Status erfahren Sie, indem Sie „Windows-Sicherheit“ über das Startmenü aufrufen und auf „Viren- & Bedrohungsschutz“ klicken.

Daten schützen

Erstellen Sie regelmäßig Backups der wichtigsten Daten (siehe S. 16). Suchen Sie im Startmenü nach „Diagnose und Feedback“ und stellen Sie sicher, dass unter „Diagnosedaten“ die Option „Standard“ aktiv ist.

Software ausmisten

Deinstallieren Sie ungenutzte Anwendungen und bringen Sie alle anderen auf den aktuellen Stand. Das gilt insbesondere für Browser und Plug-ins, Mail-Clients, Office-Programme, PDF-Viewer und Multimedia-Player.

Sicher unterwegs

In öffentlichen Netzen wie WLAN-Hotspots muss die Firewall scharf geschaltet werden, indem der PC bei der ersten Verbindung als nicht auffindbar deklariert wird. Verschlüsseln Sie Ihre Festplatte/SSD mit BitLocker (Pro-Edition von Windows) oder VeraCrypt.

Android

Smartphones und Tablets mit Android sichern

Updates installieren

Installieren Sie stets alle verfügbaren Updates, da sie Sicherheitslücken schließen. Wenn der Hersteller keine Updates mehr herausgibt, sollten Sie über die Anschaffung eines neuen Geräts nachdenken, für das es aktuelle Patches gibt.

Play Protect checken

Stellen Sie sicher, dass der vorinstallierte Virenschutz „Play Protect" aktiv ist. Sie erreichen ihn über das Menü des Play Store (Knopf oben links). Einen weiteren Virenschutz benötigen Sie nicht.

APK-Dateien meiden

Installieren Sie Apps möglichst über Google Play, da diese von Google auf Virenbefall überprüft wurden. Apps, die man als APK-Datei installiert, unterliegen dieser Prüfung nicht und sind deutlich häufiger verseucht.

Berechtigungen

Checken Sie, welche Befugnisse Sie den Apps eingeräumt haben. Unter Android 9 finden Sie diese Infos unter „Einstellungen/Apps & Benachrichtigungen/Erweitert/App-Berechtigungen". Entziehen Sie unnötige Rechte und entfernen Sie verdächtige Apps.

Sperre einrichten

Auf Ihrem Android-Gerät sind wertvolle Daten gespeichert. Nutzen Sie eine Bildschirmsperre zum Schutz vor neugierigen Blicken. Legen Sie ein Passwort oder eine PIN mit mindestens 6 Zeichen fest.

Apple iOS

iPhone und iPad bestmöglich schützen

iOS-Version checken

Stellen Sie unter „Einstellungen/Allgemein/Softwareupdate“ sicher, dass auf Ihrem Apple-Gerät die aktuelle iOS-Version installiert ist, da Updates oft auch Sicherheitslücken schließen.

Passcode & Touch ID

Das iOS-Gerät sollte beim Entsperren nach einem Passcode, Fingerabdruck oder Gesichtsscan fragen. Sie aktivieren die Displaysperre unter „Touch ID & Code“ in den Einstellungen. Nutzen Sie eine mindestens 6-stellige Ziffern- oder Zeichenfolge.

App-Berechtigungen

Überprüfen Sie unter „Einstellungen/Datenschutz“, welche Berechtigungen wie Kamera- und Mikrofonzugriff Sie Ihren Apps eingeräumt haben und deaktivieren Sie unnötige Rechte.

Zwei Faktoren

Aktivieren Sie in den Einstellungen durch einen Klick auf Ihren Namen (ganz oben) und „Passwort & Sicherheit“ die Zwei-Faktor-Authentifizierung, um Ihren Apple-Account vor Hackern zu schützen.

Backups verschlüsseln

iCloud-Backups sind nicht verschlüsselt, erstellen Sie daher am besten lokale Backups mit iTunes. Aktivieren Sie die Verschlüsselung, indem Sie in iTunes das Gerät wählen und dann auf „Übersicht/Backups/[Gerät-]Backup verschlüsseln“ klicken.

Mail

Mailen ohne Mitleser

Misstrauisch sein!

Es klingt wie eine Binse, ist aber enorm wichtig: Seien Sie bei Mails grundsätzlich skeptisch, selbst wenn Sie den Absender vermeintlich kennen. Die Absender-Adresse lässt sich leicht fälschen. Fragen Sie im Zweifel telefonisch beim Absender nach, wenn Ihnen etwas suspekt ist.

2FA aktivieren

Das Mailkonto ist der Schlüssel zu Ihrem digitalen Leben. Schützen Sie es wenn möglich per Zwei-Faktor-Authentifizierung. Das klappt etwa bei Gmail, GMX und Web.de. Dann ist zum Login ein zweiter Faktor nötig, etwa ein einmalig gültiger Code, den Sie aufs Handy geschickt bekommen.

Verschlüsselt abrufen

Wenn Sie einen Mail-Client nutzen, dann stellen Sie sicher, dass er verschlüsselt mit dem Mail-Server spricht; etwa per STARTTLS oder TLS/SSL.

Externe Inhalte

Schalten Sie im Mail-Client das Nachladen externer Inhalte aus, da Sie darüber getrackt werden können. Der Absender bekommt so etwa mit, ob und wann Sie die Mail öffnen.

Fallen vermeiden

Öffnen Sie keine ausführbaren Mail-Anhänge (auch nicht wenn sie in einem Zip-Archiv stecken). Aktivieren Sie keine Makros in angehängten Office-Dateien. Nehmen Sie sich vor Links auf Webseiten in Acht, die nach Zugangsdaten fragen.

Web-Browser

Sicher surfen

Aktuelle Version

Nutzen Sie stets die aktuelle Browser-Version, da in alten Versionen meist Sicherheitslücken klaffen. Stellen Sie sicher, dass der Browser automatisch mit Updates versorgt wird.

Erweiterungen

Browser-Erweiterungen (auch Add-ons genannt) haben Zugriff auf alle angezeigten Webseiten (auch Online-Banking). Checken Sie vor der Installation die Nutzerbewertungen.

Plug-ins meiden

Browser-Plug-ins wie Java und Silverlight sind längst überholt und potenziell unsicher. Deinstallieren Sie solche Plug-ins, wenn Sie noch welche auf Ihrem Rechner finden und nicht darauf angewiesen sind.

https:// nutzen

Steuern Sie wann immer möglich die verschlüsselt übertragene https://-Version einer Website an. Hierbei hilft die Chrome- und Firefox-Erweiterung HTTPS Everywhere (siehe ct.de/check2020). Besuchen Sie eine Site nicht, wenn der Browser einen Zertifikatsfehler anzeigt.

Berechtigungen

Websites fordern Berechtigungen an, um etwa Ihren Standort abzurufen. Erteilte Berechtigungen finden Sie bei den meisten Browsern, indem Sie in der Adressleiste links neben die Adresse klicken (meist Schloss-Symbol). Sortieren Sie alle Berechtigungen aus, die nicht länger nötig sind.

Online-Banking

Schutz für Ihre Bankgeschäfte

Phishing erkennen

Online-Betrüger verschicken massenhaft Mails im Namen von Bankinstituten, um Trojaner einzuschleusen oder Zugangsdaten abzugreifen (Phishing). Geben Sie Ihre Zugangsdaten nur auf der Webseite der Bank oder in Ihrer Online-Banking-Software ein.

Transaktion checken

Checken Sie bei Online-Überweisungen das Zielkonto und die Summe auf dem TAN-Generator, in der Banking-App oder auf dem Kartenleser und zusätzlich auf der Rechnung.

Virenfreier Rechner

Online-Banking mit dem PC ist nur sicher, wenn das System virenfrei ist. Sorgen Sie dafür, dass ein Virenscanner mit aktuellen Updates aktiv ist. Unter Windows 8.1 und 10 reicht der vorinstallierte Defender aus.

Belege überprüfen

Insbesondere Kreditkarten-Nutzer sollten regelmäßig die Abrechnung kontrollieren und unbefugte Abbuchungen umgehend an die kartenherausgebende Bank melden. Auch Ihre Kontoauszüge sollten Sie auf Auffälligkeiten untersuchen.

Handy nicht rooten

Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet nicht, da Sie damit wichtige Schutzfunktionen lahmlegen. Viele Banking-Apps starten auf modifizierten Geräten aus diesem Grund nicht.

WhatsApp

Gefahrlos chatten

WhatsApp Web

Über den PC mit WhatsApp Web zu chatten kann gefährlich sein: Einmal verknüpft, kann man über den PC dauerhaft alles mitlesen. Löschen Sie im Menü der App („Einstellungen“) unter „WhatsApp Web“ alle Geräte, die Sie nicht nutzen oder kennen.

Backup einschalten

Richten Sie in den Einstellungen unter „Chats/Chat-Backup“ das automatische Backup zu Google Drive oder in die iCloud ein, damit Chats und Medien bei einem Geräte-Crash nicht verloren gehen.

Öffentliche Infos

Standardmäßig kann jeder, der Ihre Rufnummer kennt, unter anderem Ihr Profilbild abrufen. Stellen Sie in den Einstellungen unter „Account/Datenschutz“ ein, welche Infos für wen sichtbar sein sollen.

Verifizierung

Schalten Sie die „Verifizierung in zwei Schritten“ ein, um Ihren Account durch eine sechstellige PIN zu schützen. Die PIN verhindert, dass Ihr Account übernommen werden kann. Sie finden die Funktion in den Einstellungen unter „Account“. Notieren Sie die PIN unbedingt.

Misstrauisch sein

WhatsApp ist auch bei Abzockern beliebt. Seien Sie skeptisch bei merkwürdigen Nachrichten, klicken Sie darin auf keine Links und leiten Sie die Nachrichten nicht weiter.

Social Media

Facebook, Twitter, Instagram & Co. sicher nutzen

Zwei Faktoren nutzen

Die meisten sozialen Netze bieten eine Zwei-Faktor-Authentifizierung (2FA), die Sie auch nutzen sollten. Sie erhalten dadurch beim Login einen Code aufs Handy, den Sie eingeben müssen. 2FA per App wie Google Authentificator ist sicherer als via SMS.

Verbundene Apps

Bei vielen sozialen Netzen können Sie Diensten und Apps den Zugriff auf Ihren Account gewähren. Misten Sie diese Liste regelmäßig aus und entfernen Sie alle Kandidaten, die Sie nicht länger nutzen.

Freigaben beachten

Unter anderem bei Facebook kann man festlegen, mit wem man Inhalte teilen möchte. Nutzen Sie dies, um Inhalte nur mit Personen zu teilen, die sie auch sehen dürfen.

Anfragen checken

Oft steckt hinter Freundschaftsanfragen der Versuch, persönliche Daten abzugreifen. Checken Sie jede Anfrage sorgfältig. Ist das Mitglied frisch dabei und hat viele neue Kontakte, kann es Betrug sein.

Private Nachrichten

Selbst von Nachrichten Ihrer Kontakte kann Unheil ausgehen: Hacker übernehmen Accounts und verschicken in fremdem Namen gefährliche Links oder fragen nach Geld. Seien Sie skeptisch und fragen Sie Ihren Kontakt im Zweifel über einen anderen Kanal, was es damit auf sich hat.

WLAN-Router

Schutzmaßnahmen für Fritzbox und andere

Webinterface

Sichern Sie die Konfigurationsoberfläche Ihres Routers, die Sie per Browser erreichen, durch ein individuelles Passwort. Stellen Sie sicher, dass auf dem Router stets die aktuelle Firmware installiert ist, und aktivieren Sie die automatische Update-Funktion.

WLAN sichern

Stellen Sie als Verschlüsselung ausschließlich WPA2/3 ein. Nutzen Sie ein zufälliges WLAN-Passwort mit mindestens 16 Zeichen. Aktivieren Sie den Schutz für Steuerpakete (PMF).

Gastnetz nutzen

Richten Sie für Ihre Gäste und IoT-Geräte wie den Staubsaugerroboter ein Gäste-WLAN mit separatem WPA-Passwort ein. Das klappt inzwischen mit vielen Routern.

Freigaben checken

Router können auf Wunsch Zugriffe aus dem Internet auf Geräte im Heimnetz weiterleiten (Port-Forwarding). Das macht die Geräte angreifbar, weshalb auf diesen die aktuellen Updates installiert sein müssen. Geben Sie nur Dienste der Geräte frei, die passwortgeschützt und verschlüsselt (TLS/SSL) erreichbar sind.

WPS und UPnP aus

WPS und UPnP sind Komfortfunktionen, die in der Vergangenheit immer angreifbar waren. Schalten Sie beide über das Webinterface des Routers aus.

Raspberry Pi

Großer Schutz für kleine Rechner

Passwort ändern

Ändern Sie nach der Inbetriebnahme das vorgegebene Passwort „raspberry“ des Nutzers „pi“ in ein individuelles Kennwort. Geben Sie dazu den folgenden Befehl ein: `passwd`

Updates einspielen

Installieren Sie nach Inbetriebnahme und fortan in regelmäßigen Abständen alle verfügbaren Updates für das Betriebssystem und Anwendungen. Die Befehle lauten:

```
sudo apt update
sudo apt dist-upgrade
```

Backups ziehen

Erstellen Sie regemäßig ein Backup der Speicherkarte, damit Sie im Fall eines Defekts nicht von vorn anfangen müssen. Sie können hierfür zum Beispiel einen Windows-Rechner und das Tool „Win32 Disk Imager“ (siehe ct.de/check2020) nutzen.

Skripte prüfen

Werfen Sie einen skeptischen Blick auf Shell-Befehle und -Skripte, ehe sie diese auf dem Raspi ausführen. Googeln Sie im Zweifelsfall nach der Funktion eines Befehls. Mit dem falschen Kommando können Sie das Betriebssystem zerstören.

Dienste über VPN

Nutzen Sie am besten eine VPN-Verbindung, um von unterwegs auf Server-Anwendungen wie NextCloud oder SSH zuzugreifen, die auf dem Raspi laufen. Router wie die Fritzbox lassen sich als VPN-Server nutzen.

Backup

Simple Strategien gegen Datenverlust

Machen!

Ein Backup kann im Ernstfall nur dann helfen, wenn es wirklich vorhanden ist. Raffen Sie sich auf!

Jetzt!

Am besten hilft ein Backup, wenn es aktuell ist. Das Anfertigen schreit also nach ständiger Wiederholung. Es gibt daher eine einfache Antwort auf die Frage, wann der richtige Zeitpunkt fürs nächste Backup ist: Jetzt!

Alles besser als nichts

Für den Anfang reicht das simple Kopieren Ihrer Dateien auf ein USB-Laufwerk mit dem Datei-Explorer. Das sichert Ihre Daten zwar nicht vor allen denkbaren Gefahren ab, aber vor vielen.

3-2-1-gerettet

Um Daten vor fast allen Gefahren zu schützen, beachten Sie die 3-2-1-Regel: 3 Kopien auf 2 Datenträgern unterschiedlicher Hersteller, davon 1 außer Haus. Das Original auf Ihrem Rechner zählt mit, Sie benötigen nur noch zwei weitere Kopien. Sie können zum Beispiel eine externe Festplatte und die Cloud nutzen.

Kontrolle ist besser

Nichts ist ärgerlicher, als ein Backup anzufertigen und dann erst im Ernstfall zu merken, dass dabei etwas schiefging. Also checken Sie, ob das Sichern geklappt hat – und auch, ob die Wiederherstellung funktioniert.

Passwörter

Worauf es wirklich ankommt

Kein Recycling

Nutzen Sie für jede Website und jede Anwendung ein individuelles Passwort. Wer für mehrere Websites das gleiche Passwort nutzt, ist leichte Beute: Wird eine Site gehackt, kann sich der Angreifer auch in alle anderen einloggen.

Lang statt komplex

Nutzen Sie lieber möglichst lange Kennwörter statt möglichst viele Sonderzeichen. Die Länge ist die effektivste Stellschraube, um das Knacken des Kennworts hinauszuzögern.

Passwort-Manager

Speichern Sie Ihre Passwörter auf keinen Fall unverschlüsselt auf dem Rechner. Nutzen Sie einen Passwort-Manager wie KeePass, um Zugangsdaten sicher verschlüsselt aufzubewahren. Wenn Sie Passwörter im Browser speichern, sollten Sie dafür ein Master-Passwort setzen, wenn möglich.

Zettel und Stift

Der einfachste Passwortspeicher ist ein Zettel, den Sie an einem sicheren Ort aufbewahren. Auf Geldbörse oder Tresor hat kein Trojaner Zugriff.

Zwei Faktoren

Nutzen Sie bei Webdiensten wann immer es geht die Zwei-Faktor-Authentifizierung. Dann müssen Sie beim Login einen Code angeben, den Sie etwa per SMS oder App erhalten. Das schützt Ihre Accounts selbst vor Hackern, die bereits Ihr Passwort kennen.

Impressum

Redaktion
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct.de
Chefredakteur: Dr. Jürgen Rink (jr) (verantwortlich für den Textteil)
Koordination: Ronald Eikenberg (rei@ct.de)
Art Direction: Nicole Judith Hoehne

Verlag
Heise Medien GmbH & Co. KG
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de
Herausgeber: Christian Heise, Ansgar Heise, Christian Persson
Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder
Mitglied der Geschäftsleitung: Beate Gerold, Jörg Mühle
Verlagsleiter: Dr. Alfons Schräder
Anzeigenleiter: Michael Hanke (-167, verantwortlich für den Anzeigenteil), www.heise.de/mediadaten/ct/
Leiter Vertrieb und Marketing: André Lux (-299)

Druck: Quensen Druck+Verlag GmbH, Utermöhlestraße 9, 31135 Hildesheim

myAUDIT360

Regelmäßige Schwachstellen Analyse
EXTERNER und INTERNER IT Systeme

Reporting mit technischen Maßnahmen und zur Erfüllung der DSGVO Nachweispflicht

GRATIS Webinar!
www.hackattack.com/myAUDIT360

HACKATTACK®
we hack to protect you

be.SDx

Making the net work.

Be innovative. Be yourself. With be.SDx.

be.SDx ist die Lösung, mit der Sie die Wünsche Ihrer Kunden in zukunftssichere Netzwerke verwandeln – effizient ausgerollt, flexibel gemanagt und immer auf dem neuesten Stand.

Das Ergebnis: weniger Aufwand, besserer Service, neue Chancen.

bintec-elmeg.com

Eine Lösung von bintec elmeg