Kompact

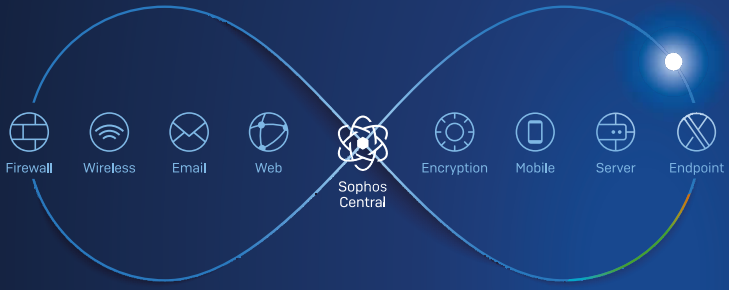
Besser geschützt in 5 Minuten

Sicherheits-Checklisten

Rundumschutz verständlich erklärt

Windows | Android | iOS | macOS | Browser | WhatsApp
Google | Social Media | Raspberry Pi | WLAN-Router
Smart Home | NAS | Backup-Strategien | Sichere Passwörter

Sophos Central
Synchronized Security



Sicherheitslösungen, die miteinander sprechen

- Echtzeitaustausch von Informationen zwischen Endpoints und Firewall
- Zentrale Verwaltung aller Sophos-Produkte
- Automatische und schnelle Reaktion bei Sicherheitsvorfällen

Koordinierte Abwehr modernster Bedrohungen.
Schnell. Einfach. Effizient.

Kostenlos testen:
www.sophos.de/central

SOPHOS
Cybersecurity made simple.

Liebe Leserinnen und Leser,

meist reichen wenige Handgriffe, um Smartphone, PC, Router & Co. vor den größten Bedrohungen zu schützen. Diese Handgriffe finden Sie als leicht verständliche Checklisten auf den folgenden Seiten. Damit können Sie nicht nur Ihre eigenen Geräte und Accounts im Handumdrehen absichern, sondern auch Freunden, Verwandten und Kollegen helfen. Geben Sie dieses Heft gern auch weiter.

Inhalt

Zu jeder Checkliste finden Sie eine ausführliche Erklärung in der **c't-Ausgabe 20/2018**. Außerdem haben wir zu allen Themen weiterführende Artikel unter **https://ct.de/check2018** für Sie hinterlegt.

Eine sichere Zeit wünscht Ihnen

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 „Defender“ ins Startmenü tippen und das Windows Defender Security Center öffnen.

Daten schützen

Erstellen Sie regelmäßig Backups der wichtigsten Daten (siehe S. 20). Suchen Sie im Startmenü nach „Datenschutzeinstellungen für Feedback“ und stellen Sie sicher, dass unter „Diagnosedaten“ die Option „Einfach“ 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 das Netz bei der ersten Verbindung als „Öffentlich“ 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 Ihren Apps eingeräumt haben. Unter Android 8 etwa finden Sie diese Informationen unter „Einstellungen/Apps & Benachrichtigungen/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 (oben links) 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.

macOS

MacBook, iMac & Co. sicher einstellen

Mac aktualisieren

Installieren Sie im App Store alle verfügbaren Updates. Aktivieren Sie in „Systemeinstellungen/App Store" den Punkt „Systemdatendateien und Sicherheitsupdates installieren". Gestatten Sie in Systemeinstellungen/Allgemein nur die Installation von Apps aus dem Mac App Store und von verifizierten Entwicklern.

Daten schützen

Um Dritte von Ihrem Mac fernzuhalten, schalten Sie in Systemeinstellungen/Benutzer/Anmeldeoptionen die „automatische Anmeldung" ab. Wechseln Sie in die FileVault-Rubrik und aktivieren Sie FileVault, um den Festspeicher zu verschlüsseln. Legen Sie regelmäßig Backups an, etwa mit Time Machine.

Privatsphäre

Erlauben Sie in Sicherheit/Privatsphäre nur erwünschten Programmen Zugriff auf Ihre Daten. Auf Mojave: Prüfen Sie die Freigaben für Fotos, Kamera und Mikrofon.

Netzwerksicherheit

Aktivieren Sie die Firewall. Gestatten Sie nur „integrierter" und „signierter Software" eingehende Verbindungen. Schalten Sie in „Weitere Optionen" den Punkt „Administratorpasswort für den Zugriff auf systemweite Einstellungen verlangen" ein. Nutzen Sie unterwegs zum Surfen die Hotspot-Funktion Ihres Smartphones oder VPN-Dienste.

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/check2018). 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.

it sa 2018

Die IT-Security Messe und Kongress

HOME OF IT SECURITY

MEIN UNTERNEHMEN EXPANDIERT MIT SICHERHEIT*

DANIEL CASE, CISO

* 2018 erwarten Sie noch mehr Aussteller und Produkte – Profitieren Sie von Europas größtem Ausstellerspektrum.

Sichern Sie sich jetzt Ihr Gratis-Ticket!

Nürnberg, Germany

9.-11. Oktober 2018

it-sa.de

NÜRNBERG MESSE

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 (Knopf mit drei Punkten) 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.

Google-Account

Account-Daten vor Hackern schützen

Zwei Faktoren nutzen

Aktivieren Sie die Zwei-Faktor-Authentifizierung (siehe ct.de/check2018), um den Account besser vor Fremdzugriff zu schützen. Sie müssen dann beim ersten Login auf einem Gerät einen Anmeldecode eingeben, den Sie etwa per SMS oder App erhalten.

Sicherheitsereignisse

Prüfen Sie unter ct.de/check2018 die Sicherheitsereignisse auf auffällige Anmeldungen. Stoßen Sie dabei auf eingeloggte Geräte, die sich nicht zuordnen können, entfernen Sie diese.

App-Berechtigungen

Überprüfen Sie unter ct.de/check2018, welche Apps und Dienste Zugriff aufs Google-Konto haben. Misten Sie die Liste gründlich aus, indem Sie unnötige Rechte entfernen.

Privatsphäre checken

Führen Sie unter ct.de/check2018 den Privatsphärecheck durch, um viele relevante Datenschutzeinstellungen zu überprüfen und anzupassen. Dort können Sie etwa den Standortverlauf konfigurieren, der es Google erlaubt, dauerhaft den Gerätestandort aufzuzeichnen.

Kontorettung

Stellen Sie sicher, dass eine zweite Mail-Adresse und Ihre Telefonnummer im Account hinterlegt sind. Damit verschaffen Sie sich Zugriff auf den Account, wenn Sie ausgesperrt sind.

Bundesamt
für Sicherheit in der
Informationstechnik

Ins Internet – mit Siche

www.bsi-fue

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

www.bsi-fuer-buerger.de • www.facebook.com/bsi.fuer.buerger

rheit!

Klick dich fit!

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.

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/check2018) 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.

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 mit AES ein (auch „WPA2 only/AES“ oder „WPA2 CCMP“). Nutzen Sie ein zufälliges WLAN-Passwort mit mindestens 16 Zeichen.

Gastnetz nutzen

Richten Sie für Ihre Gäste und IoT-Geräte wie den Staubsaugerroboter ein Gäste-WLAN mit separatem WPA2-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 verschlüsselt über 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.

secIT by Heise

HANNOVER 2019

Save the Date
13.-14.03.2019

Dieses Jahr fand die erste secIT Hannover statt – und die Premiere ist gelungen.

Nach dem tollen Start mit über 1.000 Teilnehmern und ausverkauften Ausstellungsflächen, steht für das kommende Jahr bereits jetzt die Neuauflage fest. Am **13. und 14. März 2019** findet die zweite secIT statt, diesmal in der größeren Eilenriedehalle (3.500qm) im HCC:
www.sec-it.heise.de

Heise Medien

heise Events

Smart Home

Das Zuhause sicher vernetzen

Passwörter ändern

Ändern Sie alle vom Hersteller voreingestellten Passwörter. Diese sind oft bei allen Geräten identisch oder erratbar.

Firmware

Die Hersteller von Smart-Home-Geräten schließen immer wieder Sicherheitslücken durch Firmware-Updates. Stellen Sie sicher, dass auf Ihren Geräten stets die aktuelle Firmware aktiv ist und schalten Sie wann immer möglich die automatische Update-Installation ein.

Fernzugriff

Nutzen Sie die vom Hersteller vorgesehenen Wege, um aus der Ferne auf Ihre Smart-Home-Geräte zuzugreifen. Machen Sie möglichst keine Dienste der Geräte über eine Port-Weiterleitung im Router von außen zugänglich.

Richtig vernetzen

Vernetzen Sie sicherheitsrelevante Smart-Home-Geräte wie Alarmanlagen und Kameras möglichst per Kabel, da Funkstrecken störungsanfällig sind. Richten Sie für WLAN-Komponenten möglichst ein Gastnetz ein.

Datenlecks schließen

Viele Smart-Home-Geräte und dazugehörige Apps erfassen und verschicken Daten über Ihr Nutzungsverhalten. Oft kann man die Übertragung abschalten. Durchsuchen Sie die Einstellungen nach einer entsprechenden Option und schalten Sie diese ab.

NAS

Schutz für Netzwerkspeicher

Sichere Passwörter

Schützen Sie den Zugriff auf das Webinterface mit einem individuellen Admin-Passwort. Erstellen Sie für andere Nutzer und Zwecke eingeschränkte Konten – etwa für den Medienzugriff.

Auto-Updates

Stellen Sie sicher, dass auf dem NAS die aktuelle Firmware installiert ist und aktivieren Sie die automatische Update-Funktion, sofern verfügbar.

Funktionen aus

NAS bieten viele Funktionen und arbeiten teilweise auch als Server für verschiedene Zwecke – etwa als Webserver. Aktivieren Sie nur NAS-Anwendungen, die Sie tatsächlich nutzen und halten Sie diese aktuell. Machen Sie keine NAS-Anwendungen übers Internet zugänglich.

Logging aktivieren

Wenn sich das NAS bei Fehlern per Mail oder Push-Nachricht bemerkbar machen kann, schalten Sie diese Funktion ein. So bleiben Sie über Festplattendefekte und fehlgeschlagene Login-Versuche auf dem Laufenden. Aktivieren Sie zudem das Systemlog.

Verschlüsselung

Aktivieren Sie die Laufwerksverschlüsselung, sofern unterstützt. Dann fragt das NAS nach jedem Neustart nach dem Passwort zur Entschlüsselung. Sollte das NAS mal geklaut werden, kommt der Dieb so nicht an Ihre Daten.

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, davon 1 außer Haus. Eine simple Form der Umsetzung ist, eine Kopie der Dateien auf der lokalen Platte und zwei weitere auf zwei USB-Laufwerken zu speichern, von denen Sie eines etwa bei Verwandten oder am Arbeitsplatz parken.

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 Recyling

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: Goldschmidt GmbH, Josefstraße 35, 49809 Lingen

Infoline 0800 20 60 900
www.hackattack.com/myAUDIT

myAUDIT
Vulnerability Management as a Service

Regelmäßige Schwachstellen Analyse
EXTERNER und INTERNER IT Systeme

Reporting mit technischen Maßnahmen und zur Erfüllung der DSGVO Nachweispflicht

GRATIS Webinar jetzt anmelden!
www.hackattack.com/myAUDIT

HACKATTACK®
we hack to protect you

Vertrauenswürdige IT-Sicherheit made in Germany

Wir sind immer da aktiv, wo viel auf dem Spiel steht. Wo sensible Daten und Identitäten elementare Werte von Behörden und Unternehmen sind. Wo Kunden in Sicherheitsfragen vor komplexen Herausforderungen stehen.

Unsere Spezialisten schützen Staat, Gesellschaft und Wirtschaft zuverlässig vor Cyberbedrohungen. Wir haben die IT-Sicherheitslösungen für digitale und vernetzte Infrastrukturen – und das bis zu höchsten Anforderungen an die Vertraulichkeit.

www.secunet.com

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland