SECURITY BEST PRACTICES

Praktische Cybersecurity-Empfehlungen auf Basis der Leitlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Bundesamt für Sicherheit in der Informationstechnik

BDSW

INHALT

Präsident BDSW - Werner Landstorfer

VORWORT

Die digitale Transformation prägt heute nahezu alle Bereiche unseres beruflichen und privaten Lebens. Mit ihr wachsen jedoch nicht nur Effizienz und Komfort, sondern auch die Herausforderungen im Bereich der Cybersicherheit. Angriffe auf IT-Systeme nehmen kontinuierlich zu und betreffen längst nicht mehr nur große Organisationen, sondern ebenso kleine und mittelständische Unternehmen sowie Privatpersonen.

Die Erfahrung zeigt, dass viele erfolgreiche Cyberangriffe nicht auf hochkomplexe technische Schwächen zurückzuführen sind, sondern auf vermeidbare Versäumnisse im Alltag. Fehlende Updates, unsichere Passwörter oder ein unkritischer Umgang mit digitalen Diensten bieten Angreifern oft bereits ausreichende Ansatzpunkte.

Dieses Booklet verfolgt daher ein klares Ziel: praxisnahe, verständliche und unmittelbar umsetzbare Empfehlungen bereitzustellen, die sich an den Leitlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientieren. Im Fokus stehen grundlegende Schutzmaßnahmen, die mit überschaubarem Aufwand einen erheblichen Beitrag zur Reduzierung von Cyberrisiken leisten können.

Cybersicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Sie erfordert sowohl technische Maßnahmen als auch ein entsprechendes Bewusstsein im täglichen Umgang mit digitalen Systemen. Mit den vorliegenden Empfehlungen möchten wir dazu beitragen, dieses Bewusstsein zu stärken und die digitale Resilienz nachhaltig zu verbessern.

Werner Landstorfer
Präsident des BDSW

ZIELSETZUNG

Vorsitzender BDSW-Fachausschuss Cybersicherheit
Dirk H. Bürhaus

Fachausschuss Cybersicherheit des BDSW – Verantwortung und Schutz in der digitalen Welt

Moderne Sicherheitsunternehmen übernehmen längst nicht mehr nur physische Schutzaufgaben – sie sind zunehmend Teil komplexer digitaler Infrastrukturen. Ob im Werkschutz, in Leitstellen, bei der Objektüberwachung oder im Veranstaltungsbereich: Überall bestehen digitale Schnittstellen, über welche Sicherheitsunternehmen und ihre Mitarbeitenden potenziell Angriffsfläche für Cyberkriminelle bieten. Ein unachtsamer Klick, ein ungeschütztes mobiles Gerät oder eine Nachlässigkeit im Schutz von Zugriffen und Passwörtern können weitreichende Folgen haben – nicht nur für das eigene Unternehmen, sondern auch für die Kunden, deren Schutz unsere zentrale Aufgabe ist.

Der Fachausschuss Cybersicherheit des BDSW wurde gegründet, um dieser Entwicklung aktiv zu begegnen. Ziel des FA ist es, die Mitgliedsunternehmen für die wachsende Bedeutung von Informations- und IT-Sicherheit zu sensibilisieren, praxisorientierte Handlungsempfehlungen zu erarbeiten und die Branche beim Aufbau robuster Sicherheitsstrukturen zu unterstützen. Cybersicherheit ist kein technisches Zusatzthema, sondern ein zentrales Element unternehmerisch verantwortungsvollen Handelns in der Sicherheitswirtschaft.

Sicherheitsunternehmen tragen hierbei eine besondere Verantwortung: Ihre Mitarbeitenden sind häufig in sensiblen Bereichen tätig wie z.B. in Behörden, in kritischen Infrastrukturen, in Industrie- oder Verwaltungsstandorten. Schon kleine Nachlässigkeiten, wie das Verwenden unsicherer Passwörter oder der leichtfertige Umgang mit diesen, die Nutzung privater Geräte im Kundenobjekt oder das Vernachlässigen von IT-Sicherheitsregeln beim Kunden, können Einfallstore für Cyberangriffe öffnen. Gleichzeitig werden Sicherheitsdienstleister selbst zunehmend Ziel von Attacken, um Zugang zu Kundendaten, Sicherheits- und Gebäudeplänen oder prozessualen Abläufen zu erlangen.

Der Fachausschuss setzt genau hier an. Er fördert den Austausch unter Experten, entwickelt Schulungen und Informationskampagnen und stellt konkrete Unterstützungsangebote bereit – von Tipps zum Schutz mobiler Endgeräte bis zur Sensibilisierung von Mitarbeitenden. Ziel ist es, Cybersicherheit als festen Bestandteil jeder Sicherheitsdienstleistung zu verankern.

Denn wer Sicherheit anbietet, muss selbst sicher handeln. Nur wenn die Branche selber auch im digitalen Raum glaubwürdig geschützt ist, kann sie das Vertrauen ihrer Kunden dauerhaft rechtfertigen und stärken. Der FA Cybersicherheit versteht sich dabei als Partner der Unternehmen – praxisnah, kompetent und mit dem gemeinsamen Ziel, die Sicherheitswirtschaft fit für die digitale Zukunft zu machen.

Dirk. H. Bürhaus
Vorsitzender des BDSW-Fachausschusses
Cybersicherheit

EINFÜHRUNG

Digitale Technologien sind aus dem beruflichen und privaten Alltag nicht mehr wegzudenken. Mit Computern, Smartphones und Cloud-Diensten ist es einfacher, miteinander zu kommunizieren; sie ermöglichen flexibles Arbeiten und einen schnellen Zugriff auf Informationen. Die fortschreitende Digitalisierung bringt es mit sich, dass wir immer abhängiger von IT-Systemen werden – und damit steigt das Risiko von Cyberangriffen, Schadsoftware und Datenmissbrauch.

Seit vielen Jahren weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hin, dass die meisten erfolgreichen Angriffe nicht auf hochentwickelte technische Mittel zurückzuführen sind. In der Praxis werden oft bekannte Schwachstellen, das Fehlen von Sicherheitsupdates oder einfache Versäumnisse ausgenutzt. Auch menschliche Aspekte sind hierbei von großer Bedeutung, wie der Umgang mit Passwörtern oder eine unkritische Nutzung digitaler Dienste.

Besonders relevant ist dabei:

- **Viele erfolgreiche Angriffe erfordern keine ausgeklügelten Exploits, sondern nutzen menschliche Fehler oder Nachlässigkeit**
- **Grundlegende Präventivmaßnahmen verringern das Risiko erheblich**
- **IT-Sicherheit ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess**

Deshalb ist die Sicherheit der IT keine Aktion, die man einmal durchführt, sondern ein kontinuierlicher Prozess. Sie umfasst nicht nur technische Lösungen, sondern auch organisatorische Prozesse und das Verhalten der Nutzerinnen und Nutzer. Dieser Leitfaden hat das Ziel, klare und alltagsfreundliche Empfehlungen zu bieten, um Cyberrisiken wirksam und mit wenig Aufwand zu minimieren.

Die wichtigsten Grundprinzipien der IT-Sicherheit sind:

· der Schutz von Benutzerkonten
· die regelmäßige Aktualisierung von Systemen und Anwendungen
· die Sicherung von Netzwerken
· der Einsatz von Virenschutz und Firewall
· ein bewusster Umgang mit digitalen Geräten

SCHUTZ VON BENUTZERKONTEN

Benutzerkonten sind heute der zentrale Zugang zu digitalen Diensten – und damit auch zu vielen sensiblen Informationen. Genau deshalb stehen sie besonders häufig im Visier von Cyberangriffen. Wird ein Konto kompromittiert, können Angreifer beispielsweise E-Mails lesen, auf Cloud-Speicher zugreifen oder interne Systeme missbrauchen. In der Praxis reicht oft schon ein einzelnes kompromittiertes Konto aus, um weitere Angriffe vorzubereiten oder auszuweiten.

Besonders problematisch ist die Wiederverwendung von Passwörtern. Gelangen Zugangsdaten bei einem Dienst in falsche Hände, werden sie häufig automatisiert auch bei anderen Plattformen getestet Plattformen ausprobiert.

Starke Passwörter verwenden

Ein gutes Passwort ist ausreichend lang, individuell und nicht leicht zu erraten. Das BSI empfiehlt die Nutzung von Passphrasen oder komplexen Kombinationen aus Buchstaben, Zahlen und Sonderzeichen.

Bewährte Maßnahmen sind:

- **für jeden Dienst ein eigenes Passwort zu verwenden**
- **Passwortmanager zur sicheren Verwaltung nutzen**
- **wo möglich eine Zwei-Faktor-Authentifizierung (2FA) zu aktivieren**

Die Zwei-Faktor-Authentifizierung ergänzt das Passwort um einen zusätzlichen Sicherheitsfaktor. Selbst wenn ein Passwort bekannt wird, lässt sich ein unbefugter Zugriff dadurch in vielen Fällen verhindern.

Wie sicher ist dein Passwort und wie lange dauert es, es zu knacken?

Wie lange dauert es ein Passwort zu knacken?

Anzahl der Zeichen	nur Zahlen	Kleinbuchstaben	Groß- und Kleinbuchstaben	Zahlen, Groß- und Kleinbuchstaben	Zahlen, Groß- und Kleinbuchstaben, Symbole
4	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt
5	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt
6	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt	sofort geknackt
7	sofort geknackt	sofort geknackt	1 Sekunde	2 Sekunden	4 Sekunden
8	sofort geknackt	sofort geknackt	28 Sekunden	2 Minuuten	5 Minuten
9	sofort geknackt	3 Sekunden	24 Minuten	2 Stunden	6 Stunden
10	sofort geknackt	1 Minute	21 Stunden	5 Tage	2 Wochen
11	sofort geknackt	32 Minuten	1 Monat	10 Monate	3 Jahre
12	1 Sekunde	14 Stunden	6 Jahre	53 Jahre	226 Jahre
13	5 Sekunden	2 Wochen	332 Jahre	3.000 Jahre	15.000 Jahre
14	52 Sekunden	1 Jahr	17.000 Jahre	202.000 Jahre	1 Mio. Jahre
15	9 Minuten	27 Jahre	898.000 Jahre	12 Mio. Jahre	77 Mio. Jahre
16	1 Stunde	713 Jahre	46 Mio. Jahre	779 Mio. Jahre	5 Mrd. Jahre
17	14 Stunden	18.000 Jahre	2 Mrd. Jahre	48 Mrd. Jahre	380 Mrd. Jahre
18	6 Tage	481.000 Jahre	126 Mrd. Jahre	2 Bio. Jahre	26 Bio. Jahre

Quelle: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Ein gutes Passwort muss nicht kompliziert aussehen – es muss nur lang und einzigartig sein. Passphrasen wie „Correct-Horse-Staple92!“ sind leicht zu merken und schwer zu knacken.

GRUNDSCHUTZ FÜR COMPUTER UND MOBILE GERÄTE

Ob Laptop, Smartphone oder Tablet, diese Geräte enthalten oft weit mehr sensible und persönliche Daten, als wir uns dessen bewusst sind. Deshalb ist es besonders wichtig, sie zu bewahren, als könnte man sie jederzeit verlieren.

Typische Risiken

- **Verlust oder Diebstahl des Geräts**
- **Malware-Infektion**
- **unbefugter Zugriff**
- **Missbrauch von gespeicherten Passwörtern oder Zugangsdaten**

UPDATES

Updates sind weit mehr als nur lästige Benachrichtigungen; sie sind eine der wichtigsten Sicherheitskomponenten. Jede Software und App hat Schwachstellen, und sobald diese bekannt werden, werden Angreifer sie ausnutzen. Geräte, die nicht auf dem neuesten Stand sind, laden Böswillige dazu ein, sie zu hacken - es ist wie eine unverschlossene Tür zum Netzwerk.

Warum Updates so wichtig sind

- **Viele Angriffe nutzen bekannte Schwachstellen aus, für die es schon lange Updates gibt**
- **Automatisierte Angriffe scannen gezielt nach ungepatchten Systemen**
- **Ein einziges fehlendes Update kann ausreichen, um ein ganzes Netzwerk zu gefährden**

Was oft übersehen wird

- Smart Home-Geräte wie Kameras, Türsensoren oder intelligente Steckdosen benötigen ebenfalls Updates
- Router-Firmware wird oft jahrelang nicht aktualisiert
- Einige Programme aktualisieren sich nicht automatisch, auch wenn die Option vorhanden ist

Praktische Tipps, um auf dem neuesten Stand zu bleiben

- **Aktiviere automatische Updates, wenn möglich**
- **Regelmäßig überprüfen, ob Router ein Firmware-Update benötigen**
- **Entferne veraltete Software, die keine Updates mehr erhält (sogenannte End-of-Life)**

Welche Komponenten müssen regelmäßig aktualisiert werden

- **Betriebssysteme (Laptop, Handy, Tablet)**
- **Webbrowser**
- **Anwendungen**
- **IoT-Geräte**
- **Netzwerkgeräte wie Router**
- **Smartwatches**

NETZWERKSICHERHEIT

Ein sicheres Netzwerk ist das stabile Fundament, ohne das auch die beste und neueste Software der nächsten Generation und ein starkes Passwort nur bedingt helfen. Vor allem das heimische WLAN ist ein beliebtes Einfallstor, wenn es schlecht konfiguriert ist.
Ein sicheres Netzwerk schützt Geräte vor unbefugtem Zugriff und verhindert das Abfangen sensibler Daten.

Zusätzliche Sicherheitsmaßnahmen für dein Netzwerk

- Aktiviere das Gästenetzwerk: Besucher/innen nutzen dann ein separates Wi-Fi-Netzwerk und haben keinen Zugriff auf private Geräte.
- Starte den Router regelmäßig neu: Klingt banal, aber es hilft gegen bestimmte Arten von Angriffen und stabilisiert die Updates.
- Standardpasswörter ändern
- Aktiviere die Firewall-Option im WLAN
- WPA2 oder WPA3 Verschlüsselung verwenden

Öffentliches Wi-Fi

Nutze öffentliches Wi-Fi NUR, wenn es absolut KEINE andere Möglichkeit gibt und du so schnell wie möglich eine Verbindung brauchst, aber:

- Greife nie auf Online-Banking oder sensible Konten in offenen WLANs zu.
- Überprüfe HTTPS-Verbindungen (Schlosssymbol im Browser).
- Verwende VPN.

VIRENSCHUTZ

Die meisten modernen Sicherheitsprogramme erkennen inzwischen nicht nur bekannte Malware, sondern überwachen auch verdächtiges Verhalten. Trotzdem bleiben sie eine ergänzende Komponente, kein vollständiger Schutz.

Was eine gute Sicherheitssoftware heute können sollte

- **Ransomware-Erkennung**
- **Schutz vor Phishing-Webseiten**
- **Überwachung von USB-Geräten**
- **Warnung vor unsicheren Netzwerken**
- **Erkennung bösartiger Dateien**

Wichtig - Ein veraltetes Antivirenprogramm bietet kaum Schutz.

UMGANG MIT INFIZIERTEN SYSTEMEN

Wenn ein Gerät kompromittiert wird, ist die Zeit entscheidend und jedes Detail zählt. Unüberlegte Schritte wie ein Neustart oder eine erneute Verbindung mit dem WLAN können den Schaden drastisch erhöhen.

So erkennst du eine mögliche Infektion

- Plötzlich langsames System
- Neue Programme oder Browsererweiterungen ohne Erklärung
- Unerklärliche Werbung oder Weiterleitungen im Browser
- Programme starten nicht mehr oder stürzen ab
- Verschlüsselte Dateien

Was du außerdem tun kannst

Wenn es sich um ein Firmengerät oder ein privates Gerät handelt, das Zugriff auf das Arbeitskonto hat, kontaktiere so schnell wie möglich deinen Administrator.

Für private Geräte

Passwörter ändern

Ändere dein Wi-Fi-Passwort, da auch Geräte im selben Netzwerk betroffen sein können.

Überprüfe, ob sich andere Geräte im Haushalt ungewöhnlich verhalten

Vollständigen Virenscan durchführen

Schadsoftware entfernen

Updates installieren

In kritischen Fällen Experten zu Rate ziehen (z. B. wenn Finanzdaten betroffen sind)

ÜBER DEN GRUNDSCHUTZ HINAUS – VON DER BASIS ZUR NÄCHSTEN STUFE

Weiterführende Aspekte der IT-Sicherheit

Die in diesem Leitfaden beschriebenen Maßnahmen und Empfehlungen bilden eine wichtige Grundlage für die alltägliche IT-Sicherheit und für die Minderung gängiger Cyberrisiken in der digitalen Welt.

Sie basieren auf praktischen Empfehlungen und gehen auf zentrale Schwachstellen ein, die häufig ausgenutzt werden, wie unzureichender Passwortschutz, fehlende Updates, unsichere Netzwerke, schlecht gesicherte Endgeräte oder unachtsamer Umgang mit digitalen Diensten. Angesichts der fortschreitenden Digitalisierung und der wachsenden Bedrohungslage besteht jedoch ein zunehmender Bedarf, Sicherheitskonzepte weiterzuentwickeln und an neue Anforderungen anzupassen.

Für Organisationen oder Anwendungsfälle mit erhöhten Sicherheitsanforderungen kann es daher ratsam sein, über diese grundlegenden Maßnahmen hinaus zusätzliche Ansätze in Betracht zu ziehen, die nicht nur der Prävention dienen, sondern auch der Früherkennung, der systematischen Bewertung und der effektiven Reaktion auf sicherheitsrelevante Vorfälle. In diesem Zusammenhang weist das BSI darauf hin, dass Informationen gesammelt, korreliert und analysiert werden sollten, um sicherheitsrelevante Ereignisse so umfassend und zeitnah wie möglich zu erkennen und angemessen reagieren zu können.

ERWEITERTE SICHERHEITSANSÄTZE IM ÜBERBLICK

Netzwerküberwachung

Neben vorbeugenden Sicherheitsmaßnahmen kann es sinnvoll sein, den laufenden Netzwerkverkehr systematisch zu überwachen. Das Ziel ist es, ungewöhnliche Aktivitäten, sicherheitsrelevante Anomalien oder Anzeichen von Angriffen frühzeitig zu erkennen. So lassen sich Vorfälle schneller einschätzen und geeignete Maßnahmen früher ergreifen.
Sicherheit endet nicht mit der Absicherung von Systemen, sondern umfasst auch die Fähigkeit, Abweichungen im Betrieb rechtzeitig zu erkennen.

Erkennung von Angriffsmustern

Cyberangriffe hinterlassen im normalen Betrieb oft erkennbare Spuren. Systeme zur Angriffserkennung helfen dabei, solche Indikatoren kontinuierlich zu überwachen und zu analysieren. Dies verbessert die Fähigkeit, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, besser einzuordnen und geeignete Gegenmaßnahmen einzuleiten.

SOC- und SIEM-Ansätze

Security Operations Center (SOC) sowie Systeme zum Security Information and Event Management (SIEM) dienen der zentralen Sammlung und Auswertung sicherheitsrelevanter Ereignisse.

Zentrale Auswertung sicherheitsrelevanter Ereignisse
In größeren oder stärker vernetzten Umgebungen kann es sinnvoll sein, sicherheitsrelevante Informationen aus unterschiedlichen Quellen strukturiert zusammenzuführen und auszuwerten. Dadurch lassen sich Zusammenhänge besser erkennen, Auffälligkeiten schneller einordnen und Reaktionsprozesse gezielter unterstützen.
Je komplexer digitale Umgebungen werden, desto wichtiger wird ein strukturierter Blick auf sicherheitsrelevante Ereignisse

ERWEITERTE SICHERHEITSANSÄTZE IM ÜBERBLICK

Penetrationstests

Penetrationstests sind eine geeignete Methode, um den aktuellen Sicherheitsstatus von IT-Systemen, Netzwerken oder Anwendungen gezielt zu bewerten. Sie helfen dabei, Schwachstellen unter realistischen Bedingungen aufzudecken, die Wirksamkeit bestehender Sicherheitsmaßnahmen zu bewerten und festzustellen, welche weiteren Maßnahmen erforderlich sind. Die regelmäßige Wiederholung solcher Tests kann dazu beitragen, das Sicherheitsniveau langfristig besser einzuschätzen und kontinuierlich zu verbessern.
Sicherheit sollte nicht einfach vorausgesetzt, sondern in angemessenen Abständen überprüft werden.

Schulungen und Sensibilisierung

Technische Sicherheitsmaßnahmen sind nach wie vor unverzichtbar, können jedoch allein keinen vollständigen Schutz gewährleisten. Ein wesentlicher Bestandteil einer wirksamen Cybersicherheit ist daher die Sensibilisierung der Mitarbeiter. Schulungen und Sensibilisierungsmaßnahmen helfen den Mitarbeitern, Risiken besser zu erkennen, verdächtige Situationen richtig einzuschätzen und sich in ihrem digitalen Alltag sicherer zu verhalten.
Bei der Cybersicherheit geht es auch darum, wachsam zu bleiben und sich im Alltag sicher zu verhalten.

Social Engineering

Beim Social Engineering nutzen Angreifer gezielt menschliches Verhalten aus, um an Informationen zu gelangen, Sicherheitsmaßnahmen zu umgehen oder böswillige Handlungen auszulösen.
Eine typische Taktik besteht darin, hinsichtlich Identität und Absichten Täuschungsmanöver anzuwenden. Umso wichtiger ist es, Mitarbeiter regelmäßig über verdächtige Kommunikationsszenarien, ungewöhnliche Anfragen und Versuche der psychologischen Manipulation aufzuklären.
Wenn technische Sicherheitsmaßnahmen nicht ausreichen, versuchen Angreifer oft, den menschlichen Faktor auszunutzen.

FAZIT

Cybersecurity basiert auf mehreren Schutzmaßnahmen, die gemeinsam wirken. Durch starke Authentifizierung, regelmäßige Updates, sichere Netzwerke und den Einsatz von Sicherheitssoftware können viele Angriffe bereits im Vorfeld verhindert werden.

Die in diesem Leitfaden beschriebenen Maßnahmen bilden nach wie vor die Grundlage jeder wirksamen Sicherheitsstrategie. Darüber hinaus können verwandte Themen wie Netzwerküberwachung, Intrusion Detection, die zentrale Analyse sicherheitsrelevanter Ereignisse, Penetrationstests sowie Schulungs- und Sensibilisierungsmaßnahmen zusätzlich zur Stärkung der Cybersicherheit beitragen. Dies steht auch im Einklang mit dem in dieser Broschüre dargelegten Grundgedanken, dass Cybersicherheit als ein fortlaufender Prozess verstanden werden sollte, der technische, organisatorische und menschliche Aspekte umfasst.

QUELLEN

Die Empfehlungen in diesem Leitfaden orientieren sich an offiziellen Veröffentlichungen und Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Vertiefende Hinweise finden Sie unter anderem hier:

BSI: Accountschutz – Online-Konten sicher nutzen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/accountschutz_node.html

BSI: Sichere Passwörter erstellen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen.html

BSI: Sicheres Schwachstellen- und Patch-Management
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_093.pdf

BSI: Sicherheitstipps für privates und öffentliches WLAN
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentliches-wlan_node.html

BSI: Checkliste – Infektion mit Schadprogrammen
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Checkliste_BSI_ProPK_Schadprogramme.html

BSI: Lage der IT-Sicherheit in Deutschland
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/lageberichte_node.html

Bundesamt
für Sicherheit in der
Informationstechnik

KONTAKTIEREN SIE UNS & ERFAHREN SIE MEHR

Für weitere Informationen zu unseren Cybersicherheits-Empfehlungen oder unseren Sicherheits-Projekten besuchen Sie unsere Website oder kontaktieren Sie uns direkt.

Hier finden Sie BDSW-Mitgliedunternehmen, die im Bereich Cybersicherheit tätig sind: https://www.bdsw.de/die-mitglieder/mitgliedsunternehmen-fuer-cybersicherheit

BDSW Bundesverband der Sicherheitswirtschaft e. V.
Friedrichstr. 153a
10117 Berlin

(030) 2757857-00
www.bdsw.de
mail@bdsw.de