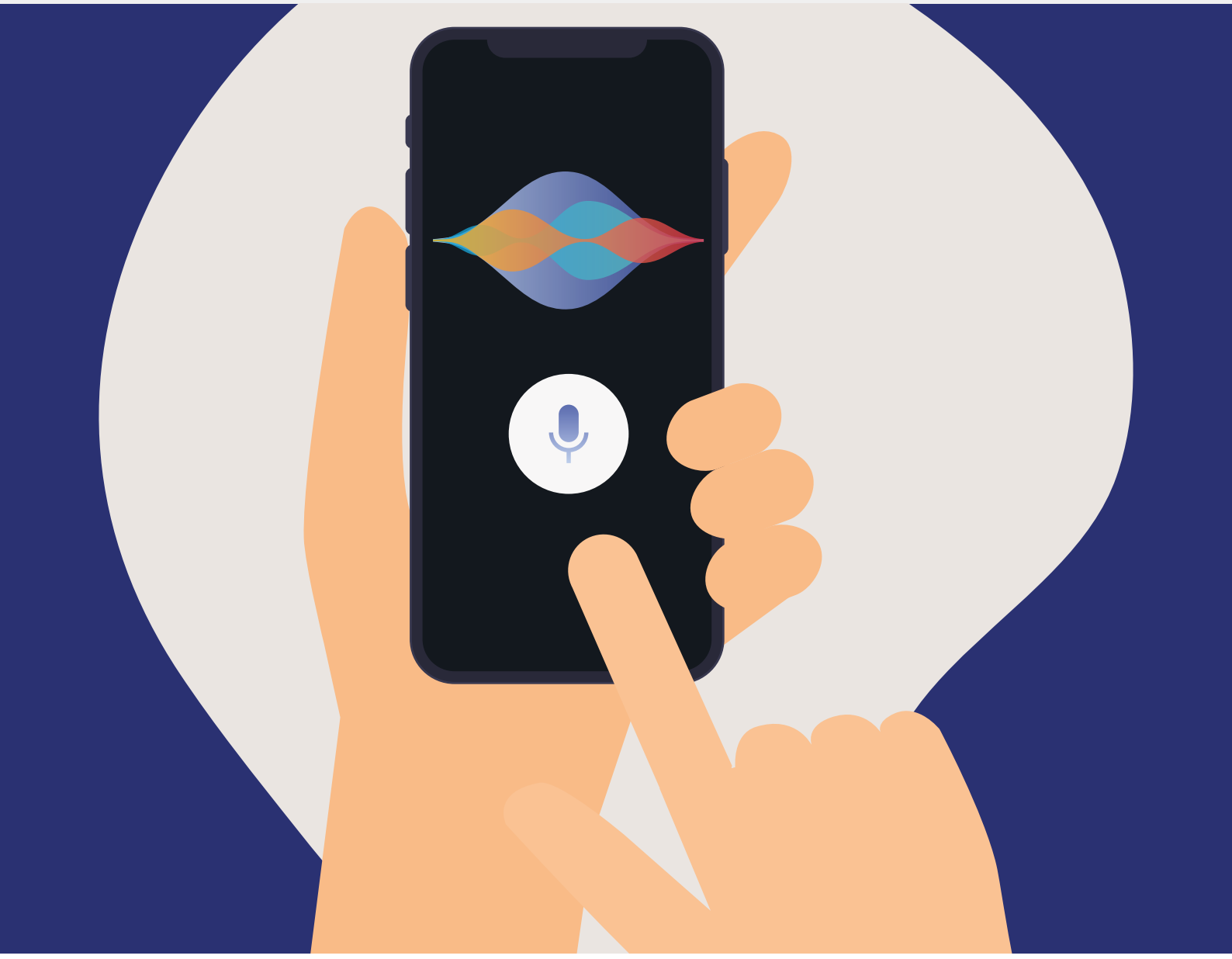
7/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER



„HEY SIRI, HÖRST DU MIT?“

Wie smarte Assistenten zum Datenschutzproblem im Büro werden

INTERNETFÄHIGE GERÄTE

Wenn der digitale Bilderrahmen 2025 zur Gefahr wird

powered by
PRIVACYXPERTS

Wenn die Technik zum Risiko wird

Liebe Leserin, lieber Leser,

digitale Helfer wie Sprachassistenten oder vernetzte Bilderrahmen erleichtern unseren Alltag – doch sie bergen auch unerkannte Gefahren. Das Bundesamt für Sicherheit in der Informationstechnik warnte kürzlich vor bis zu 30.000 digitalen Bilderrahmen in Deutschland, die mit der Schadsoftware „BadBox" ausgeliefert wurden. Diese Malware war bereits beim Kauf vorinstalliert und nutzte veraltete Android-Versionen. Sie ermöglichte es Cyberkriminellen, unbemerkt E-Mail- und Messenger-Accounts zu erstellen, Fake News zu verbreiten und die Internetverbindung der Nutzer für kriminelle Aktivitäten zu missbrauchen.

Auch im Büroalltag können smarte Assistenten zur Gefahr werden. Ein unbedachtes „Hey Siri" genügt und schon horcht KI in Gespräche hinein, für die sie nie bestimmt war. Vertrauliche Informationen, Projektinhalte oder persönliche Daten können so ungewollt aufgezeichnet oder verarbeitet werden.

Diese Beispiele zeigen, wie sehr Technik unser Leben durchdringt – und wie wichtig es ist, bewusst mit ihr umzugehen. Achtsamkeit wird zur Pflicht. Smarte Geräte sind nicht per se ein Risiko, doch sie verlangen einen bewussten Umgang. Nur so bleibt der Arbeitsplatz nicht nur digital, sondern auch datensicher.

Mit freundlichen Grüßen

Ihr Redaktionsteam von „Privacy@Work"

SEBASTIAN TAUSCH

ARBEITET ALS SELBSTSTÄNDIGER IT-BERATER UND UNTERSTÜTZT KLEINE UND MITTLERE UNTERNEHMEN PRAXISNAH IM BEREICH DATENSCHUTZ. NACH EINER KAUFMÄNNISCHEN AUSBILDUNG SAMMELTE ER VIELE JAHRE PRAKTISCHE IT-ERFAHRUNG.

ANDREAS HESSEL

IST ALS CHIEF INFORMATION SECURITY OFFICER LANGJÄHRIGER LEITER DES BEREICHES INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT EINER LANDESBANK. DANEBEN ARBEITET ER ALS EXTERNER DATENSCHUTZBEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

„HEY SIRI, HÖRST DU GERADE MIT?“ WIE SMARTE ASSISTENTEN UNBEMERKT ZUM DATENSCHUTZPROBLEM IM BÜRO WERDEN

Ein Kollege diktiert gerade eine E-Mail über ein vertrauliches Projekt. Neben ihm liegt ein privates Smartphone mit Sprachassistent. Im Hintergrund blinkt kurz die LED der smarten Uhr auf dem Handgelenk – aktiviert durch ein zufälliges Stichwort. Was nach Science-Fiction klingt, ist längst Realität im Büroalltag.

Wo KI mehr weiß, als sie sollte

Digitale Assistenten haben längst ihren Weg in unsere Arbeitswelt gefunden – oft ganz unbemerkt. Smartphones mit Siri, Uhren mit Google Assistant, smarte Lautsprecher à la Alexa oder Cortana in Windows-Geräten. Diese digitalen Helfer hören ständig mit, um bei Bedarf sofort reagieren zu können.

Mit dieser ständigen Bereitschaft beginnt das Datenschutzdilemma. Auch wenn Hersteller betonen, dass nur „nach Aktivierungswort“ aufgezeichnet wird – zahlreiche Tests und Vorfälle zeigen, dass viele Geräte zu früh oder fälschlich aktiviert werden. Und wenn das passiert, werden Gespräche nicht nur mitgehört, sondern oft auch in der Cloud gespeichert – inklusive sensibler Geschäftsdaten.

Beispiele gefällig?

- Die Besprechung in der Kaffeeküche, in der nebenbei über einen Krankheitsfall oder ein Kündigungsgespräch gesprochen wird – mit Siri aktiv im Hintergrund.
- Das Brainstorming im Büro, bei dem neue Produktideen genannt werden – mit Alexa auf dem Handy im Ladegerät.
- Der Anruf mit dem Kunden, bei dem vertrauliche Adressen, Diagnosen oder interne Informationen genannt werden – und der smarte Lautsprecher auf dem Schreibtisch blinkt auf.

Mein Tipp:

Solche Situationen sind keine Ausnahme mehr. Oft merken wir es gar nicht, wenn Geräte zuhören – denn Assistenten sind leise, unsichtbar und überall. Daher ist es wichtig, sich der Risiken bewusst zu sein.

Warum das aus Datenschutzsicht problematisch ist

Digitale Assistenten sind technisch so gebaut, dass sie ständig auf ihre Aktivierungswörter lauschen – und dabei mitunter weit mehr aufschnappen als gewünscht. Schon ein ähnlicher Klang reicht und die KI springt an: „Wie bitte?“ – mitten im Teamgespräch. In diesem Moment beginnt ein Vorgang, den man leicht unterschätzt. Das Gerät nimmt Gesprächsfetzen auf, verarbeitet sie in der Cloud, speichert sie unter Umständen dauerhaft – und niemand merkt es. Was als Komfortfunktion gedacht ist, wird so schnell zum Einfallstor für Datenschutzverletzungen – gerade dann, wenn sensible oder vertrauliche Inhalte betroffen sind.

Diese 3 Risiken sollten Sie daher kennen:

Ständige Hintergrundüberwachung: Viele Sprachassistenten sind standardmäßig so eingestellt, dass sie dauerhaft auf ein Aktivierungswort wie „Hey Siri“ oder „Okay Google“ warten. Dabei analysieren sie in Echtzeit die Umgebungsgeräusche – und speichern kurze Audioschnipsel vor dem Befehl. Auch Fehlaktivierungen sind keine Seltenheit.

1. Speicherung in der Cloud

Aufnahmen werden häufig zur Verbesserung der KI in Cloud-Rechenzentren gespeichert, teils außerhalb der EU. Das kann bedeuten:

- keine vollständige Kontrolle über die gespeicherten Daten
- möglicher Zugriff durch Dritte oder Behörden im Ausland
- Verstoß gegen die Datenschutz-Grundverordnung (DSGVO), wenn personenbezogene Daten betroffen sind

2. Fehlende Information und Einwilligung

Wenn Mitarbeitende oder Kunden nicht wissen, dass ein Gerät mithört, fehlt die Rechtsgrundlage. Eine Aufzeichnung ohne Einwilligung ist grundsätzlich nicht zulässig – auch nicht versehentlich.

3. Sensible Daten im Fokus

In vielen Unternehmen wird über besonders schützenswerte Daten gesprochen: Gesundheitsinformationen, >

> Sozialdaten, Betriebsgeheimnisse. Gelangen diese unbemerkt in eine Cloud, kann das ein meldepflichtiger Datenschutzvorfall sein – mit entsprechenden Folgen.

Was bedeutet das für Sie als Mitarbeitende? Diese Antworten müssen Sie kennen

Keine Sorge – Sie müssen Ihre smarte Uhr nicht verschrotten und auch das Smartphone darf weiter mit ins Büro. Aber es kommt auf den bewussten Umgang an.

5 wichtige Tipps, wie Sie KI-Assistenten datenschutzkonform zähmen:

1. Deaktivieren Sie den Sprachassistenten im Büro

- auf dem iPhone: „Hey Siri" unter Einstellungen > Siri & Suchen abschalten und ggf. manuell wieder einschalten.
- bei Android: Google Assistant unter Einstellungen > Google > Suche, Assistant & Sprache deaktivieren
- smarte Uhren: Mikrofon stummschalten oder den Assistenten im Menü ausschalten

Mein Tipp:
Viele Geräte erlauben auch eine gezielte Einschränkung nach Standort – z. B. nur zu Hause aktiv – oder Einstellungen nach Fokus und Uhrzeiten.

2. Keine smarten Lautsprecher im Büro oder Homeoffice-Raum

Alexa, Google Home oder ähnliche Geräte haben im beruflichen Kontext nichts verloren. Selbst im Homeoffice gilt: Schaffen Sie einen datensicheren Raum.

3. Vorsicht bei privaten Geräten im Besprechungsraum

Legen Sie Handys, Uhren oder Tablets mit Sprachassistent während vertraulicher Gespräche zur Seite, schalten Sie diese ab oder in den Flugmodus.

Mein Tipp:
Lassen Sie in sensiblen Besprechungen am besten alle Geräte mit Mikrofon ganz draußen.

4. Keine Diktate oder Memos über private Sprachassistenten

Auch wenn's bequem ist, Kundendaten oder interne Infos sollten niemals über Alexa oder Siri diktiert werden. Nutzen Sie stattdessen DSGVO-konforme Tools, die vom Unternehmen freigegeben wurden.

5. Sprechen Sie das Thema im Team an

Nicht jeder ist sich der Risiken bewusst. Helfen Sie mit, Kollegen zu sensibilisieren – ganz ohne erhobenen Zeigefinger. Vielleicht kennen Sie jemanden, der mit der Uhr am Handgelenk regelmäßig „aus Versehen" Siri aktiviert? Ein freundlicher Hinweis genügt oft schon.

KI-Tools im Büro: smart, schnell – aber bitte ohne personenbezogene Daten

Ob ChatGPT, Microsoft Copilot, Google Gemini oder NotebookLM – viele dieser KI-Werkzeuge sind längst im Büroalltag angekommen. Sie übersetzen blitzschnell, fassen lange E-Mails zusammen oder liefern Textvorschläge für den nächsten Kundenkontakt. Praktisch? Ja. Aber auch riskant, sobald personenbezogene Daten oder geschäftskritische Informationen im Spiel sind.

Denn was viele übersehen: Diese Tools arbeiten meist cloudbasiert – und was dort eingegeben wird, verlässt Ihr Unternehmen. Selbst wenn es „nur" eine E-Mail ist, in der ein Name, eine Adresse oder gar eine Diagnose steht – für den Datenschutz ist das ein potenzieller Verstoß.

Mein Tipp:
Wenn Geschäftsgeheimnisse oder vertrauliche Projektinhalte verarbeitet werden, kann daraus schnell ein ernsthafter Vorfall werden. Deshalb gilt auch hier: Nutzen Sie KI gerne für allgemeine Aufgaben – aber niemals für Inhalte mit Personenbezug oder sensiblen Unternehmensdaten. Lieber vorher kurz nachdenken als später lange erklären.

Aktuell besonders brisant: KI-Training mit echten Nutzerdaten – das sollten Sie beachten

Ein aktuelles Beispiel zeigt, wie sensibel das Thema ist. Meta (Facebook, Instagram & Co.) wird Nutzerdaten künftig für das Training seiner KI-Modelle verwenden – darunter auch öffentlich geteilte Inhalte, Chats und Fotos. Auch wenn gewisse Einschränkungen gelten, zeigt dieser Fall deutlich: Was einmal in eine Plattform

oder ein Tool eingegeben wurde, kann plötzlich ganz woanders landen.

Mein Tipp:
Gerade deshalb ist höchste Vorsicht geboten, wenn Sie personenbezogene oder interne Informationen in KI-gestützte Dienste eingeben. Denn nicht immer ist klar, wo die Daten verarbeitet werden, wie lange sie gespeichert bleiben – und wofür sie am Ende verwendet werden. Was gestern noch ein praktisches Tool war, kann morgen schon Teil eines globalen KI-Trainings sein.

Fazit: KI ist kein Spielzeug – schon gar nicht für sensible Daten

Ob smarte Assistenten wie Siri und Alexa oder moderne KI-Tools wie ChatGPT und Copilot – sie alle können den Büroalltag angenehmer und effizienter machen. Doch wo Komfort auf Vertraulichkeit trifft, ist Achtsamkeit gefragt. Denn KI hört nicht nur zu, sie merkt sich auch was – oft mehr, als uns lieb ist.

Wer im beruflichen Kontext unbedacht Informationen teilt, riskiert, dass personenbezogene Daten, Geschäftsgeheimnisse oder vertrauliche Inhalte dort landen, wo sie nicht hingehören – sei es in der Cloud, bei Dritten oder gar in Trainingsdaten künftiger KI-Modelle.

Mein Tipp:
Nutzen Sie KI als Werkzeug – nicht als Mitwisser. Schalten Sie Sprachassistenten im Büro bewusst ab und verzichten Sie bei KI-Diensten konsequent auf personenbezogene Eingaben. Dann bleiben nicht nur Ihre Daten geschützt – sondern auch das Vertrauen unserer Kunden und das Ihrer Kollegen.

Und ganz ehrlich: Die wirklich wichtigen Dinge bespricht man sowieso besser mit echten Menschen. (AH)

WENN DER DIGITALE BILDERRAHMEN 2025 ZUR GEFAHR WIRD

Internetfähige Geräte begleiten uns längst im Alltag. Selbst einfache Gadgets wie digitale Bilderrahmen oder Mediaplayer können heute über WLAN ins Internet gehen. Doch gerade diese vermeintlich „harmlosen" Geräte bergen unerwartete Risiken. So warnte kürzlich das Bundesamt für Sicherheit in der Informationstechnik vor digitalen Bilderrahmen. Der Grund hierfür war, dass bis zu 30.000 digitale Bilderrahmen ermittelt werden konnten, die mit vorinstallierter Schadsoftware ausgeliefert wurden.

Diese Malware mit dem Namen „BadBox" konnte unbemerkt Daten abgreifen und weitere Schadsoftware nachladen. Die Schadsoftware ermöglichte den Angreifern sogar Zugriff auf das Netzwerk, in dem sich entsprechend infizierte Geräte befanden. Mit anderen Worten: Ein unscheinbares Gerät auf dem Schreibtisch verwandelte sich in ein Einfallstor für Cyberkriminelle.

Vielfältige IoT-Geräte: vom Drucker bis zur Kamera

Der Begriff „Internet of Things (IoT)" – auf Deutsch „Internet der Dinge" – beschreibt ein Netzwerk aus physischen Geräten, die mit dem Internet oder einem lokalen Netzwerk verbunden sind. Im Unternehmenskontext denkt man dabei häufig zuerst an moderne Sensorsysteme oder vernetzte Maschinen in der Produktion. Doch auch alltägliche Bürogeräte können dazuzählen: Netzwerkdrucker, Multifunktionsgeräte (Drucker/Scanner/Kopierer), Smart-TVs in Besprechungsräumen, digitale Videoüberwachungssysteme oder Alarmanlagen.

All diese Geräte erfüllen ihre eigentliche Aufgabe – können jedoch gleichzeitig ein potenzielles Sicherheitsrisiko darstellen: Sie bieten mögliche Einstiegspunkte für Angreifer oder können sensible Daten ungewollt preisgeben.

Schatten-IoT: private Geräte im Firmennetz

Manchmal werden auch private IoT-Geräte ohne Wissen der IT-Verantwortlichen mit dem Firmennetzwerk verbunden. Der Fachbegriff dafür lautet „Shadow IoT" oder auf Deutsch „Schatten-IoT" – damit sind entsprechende IoT-Geräte gemeint, die ohne Wissen und Zustimmung der IT-Abteilung im Unternehmensnetz betrieben werden.

>

> Häufig handelt es sich um unscheinbare Helferlein, die Mitarbeiter auf eigene Faust installieren: etwa eine private WLAN-Steckdose, um die Bürolampe per App zu aktivieren, oder ein sprachgesteuerter Assistent (à la Alexa oder Google Home) fürs Büro, ggf. auch einfach nur, um Musik zu hören.

Die Folge: Es entstehen ***blinde Flecken*** in der IT-Sicherheit. Jedes dieser Schattengeräte stellt ein potenzielles Einfallstor dar: Weder werden sie vom IT-Team gewartet, noch erhalten sie regelmäßige Updates oder Sicherheitsprüfungen.

Sicherheitslücken durch IoT-Geräte

Angreifer können ungepatchte Schwachstellen solcher Geräte ausnutzen, um ins interne Netz vorzudringen oder den Betrieb zu stören. Je nach Einsatzbereich kann ein kompromittiertes IoT-Gerät gravierende Folgen haben – von Produktionsausfällen bis hin zu potenziell lebensbedrohlichen Situationen, etwa wenn in der industriellen Fertigung oder im Gesundheitswesen ein vernetztes System manipuliert wird.

Aber auch falls IoT-Geräte nicht mit dem Unternehmensnetzwerk verbunden sind, können diese eine Gefahr darstellen. Ein extremes Beispiel für diese Art von Risiko lieferte das Militär: So verriet ein Soldat unwissentlich den Standort eines geheimen Stützpunkts, weil seine Fitness-App die Joggingstrecke auf einer öffentlichen Onlinekarte veröffentlichte. Dieser Vorfall verdeutlicht, dass vernetzte Geräte – vom Fitnesstracker bis zur Überwachungskamera – immer auch Informationen preisgeben können, die besser vertraulich bleiben.

Weltweit sichtbar: IoT-Geräte im offenen Internet

Ein weiteres Problem mit vielen IoT-Geräten ist die oft fehlende Absicherung nach außen. Zahlreiche smarte Geräte sind über das Internet von jedermann erreichbar, sei es absichtlich – um Fernzugriff zu ermöglichen – oder durch unbedachte Voreinstellungen oder eine fehlerhafte Konfiguration.

Die spezielle Suchmaschine Shodan (https://shoadan.io) macht dieses Ausmaß eindrucksvoll deutlich. Anders als Google durchforstet Shodan nicht Webseiten, sondern scannt nach online erreichbaren Geräten wie Kameras, Steuerungen oder anderen IoT-Systemen. Dabei zeigt sich: Es ist verblüffend, welche Dinge ungeschützt im Netz gefunden werden können.

Sicherheitsforscher entdeckten über Shodan etwa frei zugängliche Steuerungssysteme für Ampelanlagen, ungesicherte Überwachungskameras und sogar die Kontrollsoftware von Industrieanlagen wie Tankstellen oder Wasserwerken.

In manchen Fällen ließen sich solche Systeme direkt bedienen, da sie entweder gar keinen Passwortschutz hatten oder bekannte – voreingestellte – Zugangsdaten verwendet wurden.

Screenshot shodan / Explore aus Mai 2025

Grundlegende Sicherheitstipps

Zum Schluss noch ein paar grundlegende Sicherheitstipps für den Umgang mit IoT-Geräten:

- **IoT-Geräte im Unternehmensnetzwerk nur mit Freigabe:** IoT-Geräte sollten nur mit Freigabe durch die IT und jeweiligen Verantwortlichen mit dem Unternehmensnetzwerk verbunden werden.
- **Standard-Passwörter ändern:** Die ab Werk gesetzten Passwörter (z. B. „admin"/„1234") sollten immer sofort durch sichere, einzigartige Kennwörter ersetzt werden. Nicht vergessen, die Passwörter sicher zu notieren, um den Zugriff auf das Gerät nicht zu verlieren!
- **Regelmäßige Updates:** Halten Sie die Firmware und Software Ihrer IoT-Geräte stets aktuell. Hersteller-Updates schließen oft bekannte Sicherheitslücken. Auch bei der Aktivierung der Update-Automatik sollte immer wieder eine manuelle Prüfung erfolgen, da die Update-Automatik durch Fehler auch ausfallen kann.
- **Geräte und Zugriffe überwachen:** Behalten Sie im Blick, welche Geräte mit Ihrem Netzwerk verbunden sind. Diesen Überblick ermöglichen teilweise

auch Router für den Heimgebrauch. Deaktivieren Sie Funktionen, die nicht benötigt werden (etwa Fernzugriff), und entfernen Sie ungenutzte Geräte aus dem Netz.
- **Netzwerksegmentierung:** Trennen Sie IoT-Geräte möglichst vom Hauptnetz, etwa durch ein eigenes WLAN für smarte Geräte. So bleiben kritische Bereiche geschützt, falls ein IoT-Gerät kompromittiert wird.
- **Security bereits beim Kauf bedenken:** Informieren Sie sich vor der Anschaffung, ob der Hersteller Sicherheitsupdates anbietet und welche Schutzfunktionen das Gerät mitbringt. Ein vermeintliches Schnäppchen ohne Support kann sich im Nachhinein als teures Sicherheitsproblem erweisen.

Zusammenfassend sollte das Thema IoT-Sicherheit nicht auf die leichte Schulter genommen werden. Schlecht abgesicherte IoT-Geräte können schnell zur „schlecht abgesicherten Hintertüre" werden und somit in das Blickfeld von Kriminellen geraten. Mit einem gesunden Bewusstsein für die Risiken und ein paar grundlegenden Maßnahmen lassen sich jedoch viele Gefahren entschärfen – damit die ***smarten*** Helfer wirklich Helfer bleiben und nicht zum trojanischen Pferd für Angreifer werden. (ST)

WUSSTEN SIE SCHON? OPERATION „ENDGAME 2.0": SCHLAG GEGEN DIE GLOBALE CYBERKRIMINALITÄT IM MAI 2025

Im Mai 2025 gelang es dem Bundeskriminalamt (BKA) und der Zentralstelle zur Bekämpfung der Internetkriminalität, gemeinsam mit internationalen Partnern einen bedeutenden Erfolg im Kampf gegen die Cyberkriminalität zu erzielen. Im Rahmen der Operation „Endgame 2.0" wurden weltweit 37 mutmaßliche Cyberkriminelle identifiziert, gegen 20 von ihnen internationale Haftbefehle erlassen und umfangreiche Maßnahmen zur Zerschlagung ihrer Infrastruktur durchgeführt. Lichtbilder und Beschreibungen einiger Beschuldigter können unter www.bka.de/endgame_fahndung eingesehen werden.

„Initial Access Malware" im Fokus

Die Operation konzentrierte sich auf sogenannte „Initial Access Malware" – Schadsoftware, die als Einstiegspunkt für komplexere Angriffe dient. Diese Malware wird von Cyberkriminellen gezielt genutzt, um Schwachstellen in IT-Systemen auszunutzen, Zugänge zu Netzwerken zu schaffen und anschließend weitere, meist sehr schwerwiegende Straftaten wie Ransomware-Angriffe oder Wirtschaftsspionage durchzuführen. Sie nutzt gezielt Sicherheitslücken in IT-Systemen, um heimlich Zugänge zu Unternehmensnetzwerken zu schaffen und damit den Weg für weitergehende Angriffe zu ebnen.

Infrastruktur zerstört, Millionen sichergestellt

Durch die Abschaltung von rund 300 Servern – davon etwa 50 in Deutschland – und die Deaktivierung von etwa 650 Domains wurde die technische Infrastruktur der Täter erheblich geschwächt. Zudem konnten Kryptowährungen im Wert von etwa 3,5 Mio. € sichergestellt werden. Diese Mittel stammen vor allem aus kriminellen Aktivitäten wie Erpressung und Betrug, die weltweit Unternehmen, Behörden und Privatpersonen geschädigt haben.

Größte Polizeiaktion gegen Cybercrime

Die Operation „Endgame 2.0" wurde 2022 von Deutschland initiiert und gilt bereits heute als größte und effektivste internationale Polizeiaktion gegen Cyberkriminalität. Im Zentrum der Maßnahmen steht die nachhaltige Zerschlagung krimineller Geschäftsmodelle – nicht nur durch Strafverfolgung einzelner Täter, sondern durch das gezielte Ausschalten ganzer Netzwerke samt Infrastruktur.

Schutz bleibt weiter notwendig

Auch wenn die Ergebnisse der Operation sehr erfreulich klingen, darf nicht übersehen werden, dass täglich neue Opfer von Angriffen bekannt werden. Unternehmen und Privatpersonen sind daher weiterhin gefordert, ihre Systeme konsequent abzusichern und IT-Sicherheitsvorgaben ernst zu nehmen. (ST)

WIE KANN ICH IT-SICHERHEITSWISSEN VERMITTELN?

Nicht jeder, der sich gut mit IT auskennt, ist auch ein guter Dozent. Vielleicht haben Sie den Auftrag bekommen, in Ihrem Unternehmen eine Auffrischung durchzuführen, und in Ihrem Kopf fangen Sie gleich an, eine PowerPoint-Präsentation mit Dutzenden von Aufzählungspunkten pro Folie zu erstellen. Sie wissen genau, dass Sie damit alle langweilen, aber Sie sind einfach kein Profi im Präsentieren. Zum Glück gibt es in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Ich habe die Ausgabe von Privacy@Work gelesen:

Name, Vorname, Abteilung	Unterschrift

Bei Fragen im Bereich Datenschutz wenden Sie sich bitte an Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten!

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autoren: Andreas Hessel, Sebastian Tausch, Produktmanagement: Lisa Greiling, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte Seite 1: Olesia_g, S. 8 Feodora – beide AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Meckenheim

Erscheinungsweise: 16-mal pro Jahr; Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier