Cybersicherheit

IT-Sicherheitskampagne „Geht mich nichts an? Mit Sicherheit!“

Zusammenfassung

1. Sicher Surfen im Internet

So verhalten Sie sich richtig:

- Recherchieren Sie nur in vertrauenswürdigen Quellen (z.B. Online-Präsenzen von renommierten Printmedien oder moderierten Lexika).
- Bleiben Sie kritisch gegenüber allen Informationen, die Sie im Internet finden.
- Fragen Sie sich immer, wer für den Inhalt verantwortlich ist und ob Sie dieser Person vertrauen können.

So schützen Sie Ihren Computer gegen den Missbrauch durch technische Webinhalte:

- Ändern Sie nicht selbstständig die Sicherheitseinstellungen Ihres Browsers (Hinweis: In den meisten Verwaltungen ist eine sichere Konfiguration des Browsers fest vorgegeben).
- Starten Sie keine Programme/Dienste aus Webseiten, sofern Sie nicht dienstlich dazu angehalten werden.
- Achten Sie auf **https://**-verschlüsselte Seiten, prüfen Sie Zertifikate für eine mögliche Verschlüsselung und vertrauen Sie nur den zertifizierten Stellen, die Sie kennen. Manchmal wird eine Fehlermeldung mit dem Hinweis angezeigt, dass ein Problem mit dem Sicherheitszertifikat einer Website vorliegt. Das Zertifikat einer Website ermöglicht das Herstellen einer sicheren Verbindung mit der Website. Zertifikatsfehler treten auf, wenn ein Problem mit einem Zertifikat oder der Verwendung eines Zertifikats durch den Webserver vorliegt. Sie sollten Zertifikatswarnungen immer genau durchlesen und nicht einfach überspringen.
- Achten Sie genau auf den „Wer-Bereich“ der Webseite (Vor dem dritten Schrägstrich einer URL, z.B. https://**achtung-falle.de**/landkreis-giessen.de/index.html) und die genaue URL. Die URL „https://marburg-biedenkopf.uniteed.de/“ führt Sie zum Beispiel nicht zum Landkreis Marburg-Biedenkopf sondern auf „uniteed.de“. Die URL „https://lkgi.de/“ führt Sie ebenfalls nicht zum Landkreis Gießen, da das erste „l“ in Wirklichkeit ein großes „i“ und kein kleines „L“ ist.

2. Umgang mit Social Media

Probleme bei Social Media

Bei der Nutzung von Social-Media-Diensten fällt eine Vielzahl von nutzerbezogenen Daten an, die für die Werbung interessant sind. Beim Besuch von Social-Media-Angeboten Dritter wird häufig auf Ihrem Computer oder Smartphone ein „Cookie“ (eine kleine Textdatei) hinterlassen, der vom Betreibenden der Seite, aber auch von Dritten, wieder ausgelesen werden kann. Über Cookies, die manchmal jahrelang gespeichert werden, ist es leicht möglich, das Surfverhalten der Besucherinnen und Besucher nachzuvollziehen.

Bei geschickter Nutzung der Cookies und anderer Daten, die Sie im Internet veröffentlichen oder unbewusst hinterlassen, besteht so die Gefahr, dass Dritte erkennen, wo Sie wie lange gesurft haben, was Sie kaufen möchten, wo Sie wohnen oder welche Hobbys Sie haben. Dies kann wiederum auch dafür genutzt werden, Sie als Angriffsziel für das sogenannte Social Engineering auszuwählen.

Wer viel über Sie weiß, dem werden Sie auch schneller vertrauen!

3. E-Mail

Zum Schutz der behördlichen Daten vor Missbrauch haben Verwaltungen oft allgemeine Richtlinien für die Verwendung von E-Mails aufgestellt, die durchaus auch für den Privatgebrauch sinnvoll sind.

Hier noch einmal die wichtigsten Regeln:

- Vertrauen Sie niemals E-Mail-Inhalten und Dateianhängen blind.
- Öffnen Sie keine Dokumente und Programme von unbekannten Absendern.
- Informieren Sie bei Verdacht auf Virenbefall Ihre IT-Ansprechperson.

- Geben Sie fehlgeleitete Informationen nicht weiter, sondern informieren Sie den Absender und löschen Sie die E-Mail.
- Nutzen Sie bei Nachrichten an mehrere externe Empfänger stets die BCC-Funktion (Blind Carbon Copy), sodass Sie externen Empfängern nicht die Daten der anderen Empfänger weitergeben.
- Falls Sie selbst eine vertrauliche E-Mail falsch versendet haben: Bitten Sie unverzüglich den oder die Empfänger um Löschung und informieren Sie Ihre Vorgesetzten sowie die IT-Ansprechperson.
- Wenn Sie eine unseriöse, seltsame oder eindeutige Phishing-Mail bekommen: nicht antworten, keinen Link anklicken, keine sensiblen Daten weitergeben, keine Anhänge oder Links öffnen.
- Senden Sie vertrauliche Daten über das Internet nur verschlüsselt. Im Zweifel fragen Sie bei Ihrer IT-Ansprechperson nach.
- Achten Sie auf „Netikette“: Verwenden Sie keine verletzenden und rechtswidrigen Inhalte.
- Bitte informieren Sie sich über die genauen Regelungen bzgl. der E-Mail-Nutzung in Ihrer Verwaltung.

4. Sichere Passwörter

Wir fassen noch mal die wichtigsten Passwort-Regeln zusammen:

- Sichere, möglichst einmalige Passwörter verwenden.
- Mindestens zehn Zeichen lang, umso mehr umso sicherer.
- Buchstaben und Zahlen sowie Groß- und Kleinschreibung sollten enthalten sein.
- Keine Passwörter aus Wörterbüchern, keine Namen, Geburtsdaten etc.

- Notieren Sie Ihr Passwort nirgendwo, außer in einem speziellen Passwortmanager.
- Geben Sie Ihr Passwort nicht an andere Personen weiter, auch nicht an Kollegen*innen.
- Seien Sie wachsam bei Anfragen nach Zugangsdaten oder Passwörtern – versucht jemand einen Social Engineering-Angriff?
- Bei Verdacht auf Social Engineering: Versuchen Sie, Sicherheit über die Identität der Person zu erlangen.

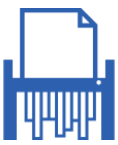
5. Umgang mit mobilen Geräten

Mobile Geräte und Datenträger stellen aufgrund ihrer Größe und Beweglichkeit ein besonderes Sicherheitsrisiko dar.

Deshalb haben die meisten Verwaltungen Regeln für den Umgang mit diesen Geräten aufgestellt, die hier sinngemäß zusammengefasst sind:

- Passwortschutz bzw. PIN-Abfrage und, wenn möglich, Verschlüsselung aktivieren.
- Mobile Datenträger immer zuerst auf Viren untersuchen.
- Mobile Geräte sicher aufbewahren.
- Für regelmäßige Software-Updates und Konfigurationsüberprüfungen sorgen.
- Nicht benötigte drahtlose Kommunikationsmöglichkeiten möglichst deaktivieren.
- Verlust von mobilen Geräten sofort der Ansprechperson und den Vorgesetzten melden.
- Keine selbstständigen Konfigurationsänderungen bei Dienstgeräten durchführen.
- Keine vertraulichen oder geheimen Daten speichern, es sei denn sie sind verschlüsselt.
- Dienstliche und private Daten nicht vermischen.

6. Umgang mit sensiblen Daten



Zum Schutz der Kundinnen und Kunden, Ihrer Verwaltung und Ihrer Kollegenschaft werden regelmäßig allgemeine Richtlinien für den Umgang mit vertraulichen Informationen aufgestellt.

Hier noch einmal die wichtigsten Regeln:

- Gesetzliche und ethische Gründe erfordern einen aktiven Daten- und Informationsschutz, und zwar von allen.
- Beachten Sie die Regelungen und Vorschriften des Datenschutz- und Informationsfreiheitsrechts und behördeninterne Regelungen.
- Vor der Weiterleitung von Informationen sind die Schutzwürdigkeit und die Empfängerliste zu prüfen.

- Besondere Vorsicht gilt bei der Verarbeitung personenbezogener Daten.
- Für Verschlusssachen (z.B. VS-NfD) gelten Spezialregelungen!
- Im Zweifel mit der Leitungsebene abstimmen!

Natürlich sind die Richtlinien nicht auf elektronisch gespeicherte Informationen beschränkt. Sie gelten genauso für den Umgang mit Papierdokumenten und sonstigen Akten.

7. Gefahren durch Viren

Computerviren: lästig – schädlich – gefährlich

Der Virenschutz hat in den letzten Jahren durch die Vielfalt von Viren immer mehr an Bedeutung gewonnen. Man kann es nur als Leichtsinn bezeichnen, sich im Internet ohne Virenschutz zu bewegen.

Täglich tauchen ca. 1.000 neue Viren auf. Deshalb kann kein aktueller Virenscanner 100%igen Schutz garantieren. Sollte einmal ein Virus nicht erkannt werden, können ein gut eingestelltes System und Ihre überlegte Reaktion den Schaden entscheidend eindämmen.

Je weniger der Virus zum Zuge kommt, desto einfacher ist es für die Verantwortlichen, den Virus zu beseitigen und so Ausfallzeiten und Kosten zu minimieren.

Hinweise:

- 100%igen Virenschutz gibt es nicht
- Aber: gute Vorsorge und richtiges Verhalten verringern mögliche Schäden!

8. Umgang mit Cloud Diensten

Cloud-Dienste sind heute Alltag. Sie bieten eine Fülle von Vorteilen, die kostengünstig eine hohe Verfügbarkeit und eine schnelle Anpassung von Kapazitäten zu niedrigen Preisen bieten.

Ihre Verwaltung wählt Cloud-Dienste sorgfältig aus und sorgt sich aktiv um die Sicherheit der Daten.

Vertrauen Sie Ihre Daten Dritten an, sollten Sie prüfen, ob die Zugangsmöglichkeiten durch den Anbieter oder andere ausgeschlossen oder zumindest nicht schädlich sind. Im Zweifelsfall gilt: Lieber die Daten zu Hause so speichern, dass nur Sie Zugang dazu haben.

Was sind Ihre Daten wert?

Wie auch bei Social Media gilt, dass der Preis, den Sie für kostenlose Dienste zahlen, Ihr Nutzungsverhalten ist beziehungsweise Ihre Daten selbst sind. Wägen Sie diese gegen (vermeintlich) günstige Angebote ab.

Hinweise:

- Verschlüsseln Sie möglichst Ihre Cloud-Daten!
- Halten Sie Kopien zu Hause vor!
- Im Zweifelsfall: Datei nicht in die Cloud.

9. Verhalten am Arbeitsplatz

Es kommt auf Sie an!

Der Schutz von Informationen der für Ihre Behörde und die Kundinnen und Kunden verwalteten Daten ist Aufgabe aller Beschäftigten.

Cybersicherheit

Jede(r) Mitarbeitende ist an ihrem/seinem Arbeitsplatz für die Informationssicherheit und den Datenschutz selbst zuständig! Falls Sie befürchten, dass einer anderen Person Ihr Passwort bekannt geworden ist, ändern Sie es unverzüglich ab.

Unter Windows sperrt z.B. die Tastenkombination **„ -Taste + L“** das System so, dass es nur durch Eingabe Ihres Passwortes oder durch eine Person mit Administratorrechten wieder benutzt werden kann.

IT-Notfallkarte


VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Verhaltenshinweise

Um wichtige Informationen in IT-Notfällen parat zu haben (zum Beispiel eine Notfallnummer), gibt es die links abgedruckten IT-Notfallkarten.

Die Notfallkarte kann – wie es bei „Verhaltensregeln im Brandfall“ oder „Fluchtweg“ üblich ist – im Büro sowie an IT-Systemen angebracht werden. Sie enthält eine individuelle Notfallnummer sowie effektive Handlungsanweisungen im Falle eines IT-Notfalls.

Sollten Sie diese noch nicht kennen bzw. erhalten haben, fragen Sie bitte Ihre IT-Ansprechpersonen.

Abschluss und Fazit

Mit diesem Flyer endet die gemeinsame Sensibilisierungskampagne „Geht mich nichts an? Mit Sicherheit!“. Alle Sicherheitstipps können sowohl auf der Lernplattform als auch auf der Webseite des Landkreises Marburg-Biedenkopf nochmals nachgelesen werden.

Das Thema Informationssicherheit endet aber nicht, sondern gewinnt mit der zunehmenden Digitalisierung immer mehr an Bedeutung und sollte das Fundament dieser Entwicklung sein.

Deshalb bleiben wir dran und möchten Ihnen eine Möglichkeit vorstellen, das gelernte Wissen regelmäßig zu aktualisieren und zu prüfen. Digital.

Interkommunale Lernplattform ILIAS

Es steht eine gemeinsame E-Learning-Plattform (Lernplattform) für alle Mitarbeitenden der teilnehmenden Städte und Gemeinde online zur Verfügung.

In Form von kurzen Lerninhalten werden dort die Inhalte aus der Sensibilisierungskampagne in digitaler Weise wiedergegeben und multimedial mit Bildern und Videos unterstützt.

Mit dem Wissen aus den neun IT-Sicherheitstipps der Kampagne oder den Inhalten des IT-Sicherheitstrainings auf der Lernplattform kann ein Abschlusszertifikat mittels Test erworben werden.

Dieses Zertifikat bescheinigt ein erfolgreich geprüftes Grundwissen im Bereich Informationssicherheit und dient dabei zwei Zwecken: als Bescheinigung für Sie als Mitarbeitende/n sowie als Nachweis der Behördenleitung über die Sensibilisierung ihrer Mitarbeitenden.

Um sich auf der Lernplattform zu registrieren folgen Sie bitte dem unten stehenden Link oder scannen Sie den QR-Code ein. Für die erstmalige Registrierung wird ein Registrierungscode benötigt. Diesen erhalten Sie bei Ihrer IT-Ansprechperson.

Wir wünschen Ihnen eine IT-sichere Zeit!