IT-Sicherheitstipp Nr.9 – November 2019

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.

Nicht nur die von Ihnen zu verarbeitenden Daten können durch Ihr Verhalten sicherheitsrelevanten Gefahren ausgesetzt werden. Durch ein Versehen oder technische Lücken könnte auch der Zugriff auf andere Datenbestände möglich werden. Daher sollten Sie – auch zu Ihrer persönlichen Absicherung – einige grundsätzliche Verhaltensregeln berücksichtigen.

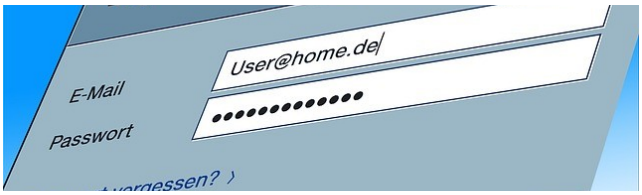
Jede(r) Mitarbeitende ist an ihrem/seinem Arbeitsplatz für die Informationssicherheit und den Datenschutz selbst zuständig!

Kriminelle suchen sich oft den leichtesten Weg und setzen dabei gezielt Social Engineering, also das Vortäuschen von falschen Identitäten und darauffolgende Manipulationsversuche ein, um an interne Daten und Systeme zu kommen.

Tipps:
- Ein Großteil der Gefahren entsteht durch Unachtsamkeit der IT-Nutzerinnen und IT-Nutzer. Arbeiten Sie daher umsichtig und sorgfältig!
- Seien Sie sich Ihrer Verantwortung für Ihren Arbeitsplatz bewusst!
- Im Zweifelsfall wenden Sie sich an Ihre IT-Ansprechpersonen. Lieber einmal zu viel fragen, als einmal zu wenig.

Regel 1: Passwörter nicht weitergeben

Ihnen anvertraute oder von Ihnen erzeugte Passwörter dürfen Sie keinesfalls weitergeben. Es ist auch verboten, sie aufzuschreiben, in Schubladen, unter Schreibtisch unterlagen oder Tastaturen o.ä. – also letztlich für Dritte zugänglich – aufzubewahren!



Gerne können Sie Ihre IT-Ansprechpersonen um Unterstützung bei der sicheren Passwortvergabe sowie auch -Aufbewahrung bitten. Mittels Passwortkarten, Passwortmanagern und Merkhilfen gibt es sichere Möglichkeiten dazu.

Passwörter sind personengebunden. Das heißt: Alle berechtigten Personen können über die zuständige Organisationseinheit ein eigenes Passwort erhalten. Eine Weitergabe Ihres Passworts ist nicht notwendig.

Tipps:
- Nutzen Sie sichere Passwörter!
- Bewahren Sie Ihr Passwort nur an sicheren Orten auf.
- Geben Sie nie ein Passwort weiter (auch nicht an Kolleginnen oder Kollegen).

Falls Sie befürchten, dass einer anderen Person Ihr Passwort bekannt geworden ist, ändern Sie es unverzüglich ab.

Weitere Informationen zu diesem Thema erhalten Sie im IT-Sicherheitstipp Nr.4 – Sichere Passwörter, erschienen im Juni 2019.

Cybersicherheit

Regel 2: Zugang sichern

Der Computer an Ihrem Arbeitsplatz ist das Tor zu den auf diesem Rechner gespeicherten Daten, aber auch zu Daten auf anderen Computern Ihrer Verwaltung und oft auch zum Internet.

Wenn Sie Ihr Büro verlassen, sollten Sie immer den Zugang zum Computersystem sperren. Dies geschieht mit einem einfachen Handgriff und verhindert, dass Dritte Zugriff auf Daten haben oder in Ihrem Namen Nachrichten schreiben.

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. In einigen Verwaltungen wird das System auch automatisch, nach einer eingestellten Inaktivitätszeit, gesperrt.

Denken Sie aber nicht nur an Ihren Computer, sondern an Ihren gesamten Arbeitsplatz. Liegen während Ihrer Abwesenheit offen Dokumente herum?

Regel 3: Social Engineering-Angriffe erkennen und abwehren

Seien Sie misstrauisch, wenn jemand Ihre Zugangsdaten, insbesondere Passwörter erfragt. Dies gilt gerade bei Ihnen Unbekannten, die auf Auskunft drängen und sich auf ihre Autorität (hoher Funktionsträger etc.) oder eine hohe Dringlichkeit („Die Zeit drängt …", „Sie behindern …") berufen.

Häufig werden gezielt Personen für Angriffe ausgewählt, die keine sicherheitsrelevanten Aufgaben haben. Über deren Zugänge zu Anwendungen und Netzwerken versuchen die Angreifer und Angreiferinnen als Sprungbrett dann weiter in die Systeme einzudringen.

Gerade bei E-Mails ist höchste Vorsicht geboten. Welche Personalstelle nimmt etwa nicht täglich Bewerbungen über E-Mail entgegen? Viele Angreifer setzen genau dort an und „bewerben" sich per E-Mail, mit Schadcode im Anhang.

Wie verhalten Sie sich, wenn Sie Zweifel haben?

- Lassen Sie sich im Zweifelfsfall eine Rückrufnummer geben, die Sie überprüfen.
- Erkundigen Sie sich bei Vorgesetzten, Kollegen oder ihren Ansprechpersonen, ob die anfragende Person vertrauenswürdig und „echt" ist.
- Geben Sie keine Zugangsdaten leichtfertig heraus.
- Versichern Sie sich der Identität der abfragenden Person.

Weitere Informationen zu diesem Thema erhalten Sie im
IT-Sicherheitstipp Nr.3 – Gefahren durch E-Mails, erschienen im Mai 2019.

Regel 4: Vorsicht bei mobilen Datenträgern

Durch USB-Sticks, Smartphones und andere mobile Datenträger können leicht Daten auf und von Computern kopiert werden. Dies birgt erhebliche Gefahren.

Zum einen ist oft nicht nachvollziehbar, welche Daten vom Computer heruterkopiert werden. Somit sind ein „Diebstahl" und die unberechtigte Verwendung von Daten möglich. Auch lassen sich kleine Geräte leichter verlieren oder stehlen.

Zum anderen besteht die Gefahr, dass auf den mobilen Geräten enthaltene Viren auf den Computer und damit in das Verwaltungsnetz gelangen.

Weitere Informationen zu diesem Thema erhalten Sie im
IT-Sicherheitstipp Nr.5 – Umgang mit mobilen Geräten, erschienen im Juli 2019.

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf
und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!

Regel 5: Verhalten bei IT-Notfällen

Sollten Sie den Eindruck haben, dass jemand durch vorsätzliches Einwirken auf Sie versucht, Passwörter, Zugangsdaten oder konkrete Inhaltsdaten zu erkunden, weisen Sie dieses Ansinnen höflich, aber bestimmt zurück und informieren Sie Ihre IT-Ansprechpersonen.

Wenn Ihnen etwas an Ihrem IT-System verdächtig vorkommt, oder Sie aus Versehen eine unseriöse E-Mail/ Datei oder einen Link angeklickt haben, bewahren Sie bitte Ruhe und kontaktieren Sie umgehend Ihre IT-Ansprechpersonen. Weitere Hinweise auf einen möglichen IT-Notfall sind:

„Mein Rechner verhält sich anders als gewöhnlich, es öffnen sich Dialogboxen, die ich nicht kenne."

„Mein Internet Browser ruft Seiten auf, die ich nicht ausgewählt habe, ich bekomme Benachrichtigungen die ich nicht zuordnen kann."

„Ich werde von mir bekannten Leuten per E-Mail kontaktiert. Die E-Mail stammt jedoch gar nicht von diesen."

„E-Mails verlinken zu Dokumenten im Internet, oder haben merkwürdige Anhänge."

„Der Rechner ist plötzlich deutlich langsamer als gewöhnlich, manche sonst verfügbaren Ressourcen lassen sich nicht aufrufen."

Ich werde nach Passwörtern an Stellen gefragt an denen das normalerweise nicht der Fall ist."

„Ich habe plötzlich Programme auf meinem Rechner die mir merkwürdig vorkommen."

„Fremde haben sich an oder in der Nähe von IT-Systemen zu schaffen gemacht"

„An meinem IT-Arbeitsplatz – oder an anderen Stellen (z.B. an den Netzwerkanschlüssen im Besprechungsraum) – sind mir unbekannte Geräte oder Kabel aufgefallen"

Falls Ihnen die Kabel des Rechners vertraut sind, trennen Sie bitte ebenfalls die Netzwerkverbindung durch Ziehen des entsprechenden Steckers oder Abschalten von WLAN- bzw. Mobilfunkverbindungen. Dadurch wird z.B. die Verbreitung eines Virus im Verwaltungsnetz verhindert. Ein typischer Netzwerkstecker sieht wie folgt aus:

Ihre Kollegen*innen aus der IT-Abteilung sind Ihnen für solche Informationen dankbar, denken Sie bitte aber auch daran, dass Ihnen der reguläre IT-Support für kleinere Störungen ebenfalls zur Verfügung steht und nicht jedes Problem ein Notfall ist.

IT-Notfallkarte

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 angebracht werden. Sie enthält eine individuelle Notfallnummer sowie effektive Handlungsanweisungen im Falle eines IT-Notfalls. Die Notfallkarten werden zukünftig bereitgestellt.

Tipps:

- Ruhe bewahren!
- Weisen Sie Fragen nach Ihren Passwörtern höflich aber bestimmt zurück.
- Melden Sie verdächtigte Vorfälle direkt Ihren IT-Ansprechpersonen und unterbrechen Sie die Arbeit am System.
- Trennen Sie die Netzwerkverbindung Ihres IT-Systems (Beispielsweise durch das Ausstecken des Netzwerksteckers oder der Deaktivierung der WLAN-Schnittstelle).
- Dokumentieren Sie Ihre Beobachtungen, solange Sie auf Hilfe warten.