DIGITAL INSIGHTS

KOMPETENZZENTRUM FÜR DIGITALISIERUNG IM LÄNDLICHEN RAUM

EINFÜHRUNG IN DIE BASICS DER IT-SECURITY

FÜNF EXKLUSIVE THEMENBLÖCKE:

- IT-Sicherheit
- Social Engineering
- Datensicherung / Backups
- Sicher im Home Office / Sicher im Netz
- Notfallplan und Verhalten im Schadensfall

Titelmotiv: Generiert mit der KI Midjourney

KDLR
Kompetenzzentrum
für Digitalisierung
im ländlichen Raum

Liebe Leserinnen und Leser,

Foto: Hessische Staatkanzlei / Diehl

gemäß Hessischem Mittelstandsbericht 2022 haben kleine und mittlere Unternehmen (KMU) mit 99,5 Prozent den größten Anteil am hessischen Unternehmensbestand. Sie prägen also insbesondere die ländlichen Räume. Allerdings schlossen laut KfW Research vom Juli 2023 nur 27 Prozent der Unternehmen mit unter fünf Beschäftigten Digitalisierungsvorhaben ab. Dies führt perspektivisch zu Nachteilen im Wettbewerb.

Hier setzt das KDLR mit Informations- und Netzwerkangeboten an, durch die gerade KMU für die Notwendigkeiten digitaler Transformation sensibilisiert und Beschäftigte qualifiziert werden sollen. Insofern wird das KDLR vor allem als Plattform und Impulsgeber fungieren. Darum ist es mir als Ministerin für Digitale Strategie und Entwicklung wichtig, es als eines der Leuchtturmprojekte in unserer Strategie „Digitales Hessen – Wo Zukunft zuhause ist“ hervorzuheben. Für den Aufbau und die Etablierung des KDLR stellen wir dem House of Digital Transformation e.V. (HoDT) bis Ende 2023 insgesamt 450.000 Euro bereit.

Mit der vorliegenden Präsentation sollen durch das KDLR erarbeitete Ergebnisse und Inhalte im Sinne des Transfers aufbereitet werden. Da Digitalisierung gemeinsam besser gelingt, wenden Sie sich gerne auch an die Geschäftsstelle des HoDT.

Gutes Gelingen

Ihre Prof. Dr. Kristina Sinemus

Hessische Ministerin für Digitale Strategie und Entwicklung
Vorstandsvorsitzende des House of Digital Transformation e.V.

Hauke Schlüter
Geschäftsführer
House of Digital Transformation
www.hodt-hessen.de

Foto: Privat

Dominque Wüst
IT Security Project Management
Micromata GmbH
www.micromata.de

Foto: Micromata

Das HoDT ist eine Plattform zur Förderung der Digitalen Transformation in Hessen. Ziel ist die Verbindung von Politik, Wissenschaft und Wirtschaft im Innovationscluster, insbesondere durch Wissenstransfer und Forschung sowie Bildung & Weiterbildung.

Zur Erhöhung des Digitalen Reifegrades von KMU und Kommunen betreibt das HoDT das KDLR | Kompetenzzentrum für Digitalisierung im ländlichen Raum, um Digitalisierungsprojekte auch auf regionale Anforderungen anzupassen und allen hessischen Regionen zur Verfügung zu stellen, sowie seit Februar 2023 mit Partnern einen European Digital Innovation Hub (EDIH).

Die Inhalte und Themen unserer Formate und Projekte stellen wir Ihnen gebündelt mit der DIGITAL INSIGHTS zur Verfügung. Weitere spannende Themen können Sie kostenlos auf unserer Webseite herunterladen.

Viel Spaß beim Lesen

Hauke Schlüter

Micromata entwickelt seit 1997 passgenaue Softwarelösungen für Unternehmen aus den Bereichen Logistik, Automotive, Medical Care, Energie und Rohstoffgewinnung. Als Softwarehaus für ganzheitliche Lösungen gehört IT-Security zu unseren zentralen Kernkompetenzen, ist sie doch eine tragende Säule einer tragfähigen Digitalisierung.

Um hier hohe Standards zu etablieren, orientieren wir uns an den Richtlinien des BSI sowie den international geltenden Best Practices des OWASP. Darüber hinaus sind wir TISAX-zertifiziert und unsere Lösungen entsprechen der deutschen ISO-Norm 27001.

Unser Ziel ist es, das Thema IT-Security stärker in den Fokus der Menschen zu rücken, aufzuklären, zu unterstützen und zu beraten. Neben unserer täglichen Arbeit für Auftraggeber aus Industrie und Handel teilen wir deshalb unser Wissen mit allen, die sich im Bereich IT-Security besser aufstellen möchten.

Viel Spaß beim Lesen!

Dominique Wüst

Motiv: Generiert mit der KI Midjourney

Über unsere Themenblöcke

Tipps und Best Practices rund um das Thema IT-Security

Auf den folgenden Seiten erhalten Sie zunächst eine Einführung in das Thema IT-Security und erfahren, welche Relevanz es hat.

Im Anschluss lesen Sie dann, welche Risiken es gibt und wie Sie sich wirksam davor schützen können.

Über die Zielgruppen

Zielgruppe dieser Ausgabe

Sie gibt Ihnen einen Einblick in die wichtigsten Themen der IT-Security, insbesondere für Unternehmen, die keine eigene IT-Abteilung haben und ohne interne Fachleute auskommen müssen. Das Dokument soll Ihnen dabei helfen, einen ersten Überblick über die aktuelle Gefahrenlage zu bekommen und mit gezielten, kleinen Maßnahmen Ihre Sicherheit zu erhöhen.

Von diesen Lösungen profitieren:

- **Soloselbstständige**
- **Kleinunternehmer:innen**
- **Mittelständische Unternehmen**

„Ein großes Dankeschön an Micromata und das KDLR, die sich mit außerordentlich viel Know-how und Engagement dafür einsetzen, dass auch IT-Laien wie mir das Thema IT-Sicherheit verständlich wird."

KMU aus dem Schwalm-Eder-Kreis

Motiv: Generiert mit der KI Midjourney

Motiv: Generiert mit der KI Midjourney

Themenblock 1

IT Sicherheit

Grundlagen und Strategie für KMU

Relevanz

Seit dem Jahr 2022 zählen Cyberattacken zu den größten Geschäftsrisiken überhaupt. Inzwischen sind Hackergruppen weltweit organisiert, investieren nicht nur in gut ausgebildete Arbeitskräfte, sondern bauen professionelle Unternehmen auf. Im Darknet gibt es zudem eine Vielzahl automatisierter Schadsoftware käuflich zu erwerben. Die jüngste Entwicklung zeigt außerdem, dass vermehrt kleine und mittelständische Unternehmen angegriffen werden – einfach, weil die Sicherheitsstandards und damit die Hürden für die Angreifer:innen hier nicht besonders hoch sind. Dabei werden diese Unternehmen entweder selbst zur Zielscheibe für Datenklau und Erpressung oder aber in ihrer Eigenschaft als Dienstleister:in oder Zuliefer:in missbraucht, um von dort in die Systeme größerer Firmen einzudringen, deren eigenes Sicherheitsprotokoll zu hart zu knacken ist.

Risiken und Gefahren

Welche Folgen Cyberangriffe für Unternehmen haben können, zeigen unzählige Beispiele aus den Nachrichten. Im Sommer 2022 legten Hacker z. B. die Kasseler Stadtreiniger lahm. Bürger:innen konnten über Wochen ihren Sperrmüll nicht mehr online anmelden und mussten auf die postalische Anmeldung zurückgreifen. Noch schlimmer traf es Ende 2022 den Großhandel Metro AG. Dort konnten die Warenwirtschaftssysteme nicht mehr genutzt werden. Dies hatte zur Folge, dass Rechnungen wieder manuell geschrieben werden mussten, die Warenbestände und Bestellungen komplett durcheinandergerieten und die Verfügbarkeit der Waren nicht mehr sichergestellt werden konnte. Beiden Unternehmen entstand durch die Angriffe ein schwerer wirtschaftlicher Schaden.

Ein erfolgreicher Angriff sabotiert nämlich die digitalen Abläufe, legt bspw. Kommunikationskanäle lahm, verschlüsselt oder klaut sensible Unternehmensdaten, bringt ganze Produktions- und Serviceprozesse zum Erliegen. Daraus folgt ein massiver wirtschaftlicher Schaden – auch dann, wenn Betroffene der Lösegeldzahlung nicht nachkommen.

So muss etwa in IT-Forensik investiert werden, um die Schwachstelle zu finden, es müssen Reparaturen vorgenommen, Daten wiederhergestellt und im schlimmsten Fall Kunden entschädigt werden. Damit einher geht ein substanzieller Reputationsverlust, der nur schwer wiedergutzumachen ist. Insbesondere bei KMU kann dies die Existenz bedrohen und sogar zur Insolvenz führen. Deshalb ist es wichtig, sich der Risiken bewusst zu sein und angemessene Präventivmaßnahmen zu etablieren. Im Folgenden werden Sie sehen, dass auch kleine Vorkehrungen Ihre IT-Sicherheit signifikant erhöhen können.

Handlungsempfehlungen

Die meisten Angriffe beginnen damit, dass Kriminelle sich Zugang zu Ihren Systemen verschaffen: durch abgefangene Passwörter, Sicherheitslücken in Anwendungen oder Manipulation von Mitarbeitenden. Oft werden verschiedene Methoden kombiniert. Es geht also darum, die Hürde für Hacker:innen so hoch wie möglich zu halten. Dies gelingt durch den Schutz der folgenden drei Bereiche:

1. Passwörter

Es gibt im Netz frei zugängliche Listen von Passwörtern, die bereits geknackt wurden. In Kombination mit ebenfalls frei zugänglichen Tools gelingt es Angreifer:innen, diese Passwörter in wenigen Sekunden durchzuprobieren – so lange, bis ein Login erfolgreich ist. Je simpler ein Passwort ist, desto einfacher ist es zu knacken.

Unsere Empfehlungen:

- Nutzen Sie starke Passwörter, die möglichst lang und abstrakt sind und keine persönlichen Informationen enthalten.

- Verwenden Sie niemals ein Passwort für mehrere Zugänge.

- Nutzen Sie Passwortmanager, um sich Ihre komplexen Passwörter zu merken.

- Nutzen Sie Passwortkarten, hier erfahren Sie mehr dazu: https://www.datenschutz.org/passwortkarte.

- Nutzen Sie Passwortgeneratoren, hier ein Beispiel: https://www.datenschutz.org/passwort-generator/.

- Sprechen Sie nicht über Ihre Passwörter und lassen Sie sie niemals offen herumliegen.

2. Patches

Stellen Sie sicher, dass Ihre Software immer auf dem aktuellen Stand ist. Wenn Softwarehersteller von einer Sicherheitslücke erfahren, stellen sie ein so genanntes Patch bereit, das diese Lücke schließt. Solche Patches werden über Updates eingespielt.

Unsere Empfehlungen:

Aktivieren Sie, wo möglich, die Funktion „Auto Update“. Viele Betriebssysteme und Browser bieten diese Option an.

- Halten Sie sich auf dem Laufenden, insbesondere bei Software, die Sie nicht automatisch updaten können. Oftmals finden Sie Informationen zu anstehenden Patches auf der Homepage des Herstellers oder Sie erhalten Benachrichtigungen über den App Store / Google Play Store.

- Laden Sie Updates nur aus vertrauenswürdigen Quellen herunter, wie zum Beispiel der Hersteller-Homepage oder dem App Store / Play Store. Installieren Sie keine Updates, die Ihnen per E-Mail zugesendet wurden.

3. Personen

- Auch der Mensch ist eine potenzielle Schwachstelle. Das nutzen Cyberkriminelle mit den Mitteln des Social Engineerings aus. Im nächsten Themenblock gehen wir tiefer darauf ein.

Motiv: Generiert mit der KI Midjourney

Themenblock 2

Manipulation statt Hacking

Wie Social Engineering uns dazu bringt, sensible Informationen freiwillig preiszugeben

Relevanz

Das BSI definiert Social Engineering als „…eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter:innen so manipuliert werden, dass sie unzulässig handeln." Menschen werden von Cyberkriminellen also dazu gebracht, Dinge zu tun, die sie nicht wollen – anfänglich, ohne es zu merken. Einfallstore für Manipulationsversuche sind hier nicht zwingend digital: Der berüchtigte Enkeltrick und ähnliche Täuschungsmanöver spielen sich zunächst am Telefon ab, falsche Polizist:innen klingeln gern mal an der Haustür. Doch natürlich sind auch die digitalen Kanäle wie E-Mail oder Social Media beliebte Kanäle für Social Engineering. Gelingt es Angreifer:innen, das Vertrauen der Betroffenen auf diesen Wegen zu erschleichen und ihre instinktive Skepsis auszuschalten, ist der Weg zu ihren persönlichen Daten und Geldbörsen nicht mehr weit. Wie oft das gelingt, zeigt die Statistik: Im März 2022 wurden weltweit gut 385.000 Phishing-Webseiten entdeckt, etwa doppelt so viele wie im Jahr davor.

Risiken und Gefahren

Phishing ist nicht die einzige Gefahr. Oftmals spielen die Angreifer:innen dem Opfer vor, eine hochrangige Person aus dem eigenen Unternehmen oder dem näheren Arbeitsumfeld zu sein und versuchen auf diese Art, vertrauliche Informationen zu erhalten. In anderen Fällen versuchen sie, ins Gebäude einzudringen, geben sich als Lieferant:in, Postbot:in oder Besucher:in aus. Social Engineering kann sehr komplex sein und kombiniert psychologische Tricks mit technischen Komponenten.

Der erste Schritt eines Angriffs dient der Informationsgewinnung, um ein realistisches Bild vom betreffenden Unternehmen zu bekommen. Im zweiten Schritt wird ein Szenario aufgebaut, das eine Kontaktaufnahme mit der Zielperson rechtfertigt. Dabei spielen den Angreifer:innen natürliche menschliche Reflexe in die Karten, etwa im Umgang mit Zeitdruck oder Hierarchien, mit Angst oder Lob und nicht selten auch einfach der Wunsch, zu helfen.

Die Kommunikation mit der Zielperson wird so lange aufrechterhalten, bis Angreifer:innen ihr Ziel erreichen, unternehmenskritische Daten oder Geld erbeutet haben. Zum Abschluss beendet sie die Interaktion, ohne einen Verdacht hervorzurufen und verwischt seine Spuren. In vielen Fällen bleiben solche Social-Engineering-Angriffe unentdeckt oder werden verschwiegen, weil es den Opfern unangenehm ist, darüber zu sprechen.

Handlungsempfehlungen

Sollten Sie den Eindruck haben, Opfer eines Social-Engineering-Angriffs geworden zu sein, oder Ihnen eine Situation verdächtig erscheint, reden Sie darüber! Verschweigen Sie solche Vorfälle nicht aus falscher Scham. Je mehr wir darüber sprechen, desto besser sind wir künftig gewappnet, um das Risiko zu verringern. In der unmittelbaren Situation gilt:

- Ruhe bewahren, nicht überstürzt reagieren.
- Bedenkzeit beanspruchen und ggf. einen Rückruf anbieten.
- Prüfen Sie die Rechtmäßigkeit der Telefonnummer oder der E-Mailadresse über einen Zweitkanal.
- Analysieren Sie: Ist das, was die Person mir erzählt, plausibel? Ist das, was sie fordert, angemessen? Suchen Sie im Zweifelsfall Rat bei Kolleg:innen.
- Geben Sie Informationen nur heraus und führen Sie Handlungen nur durch, nachdem Sie Absender:in und Anliegen sorgfältig geprüft und zweifelsfrei als zulässig klassifiziert haben.
- Geben Sie möglichst wenig über sich selbst in der Öffentlichkeit preis. Bedenken Sie, wer Urlaubs- und Familienfotos von Ihnen sehen darf, wer welche Postings lesen darf und welche Kontaktanfragen Sie annehmen.

Motiv: Generiert mit der KI Midjourney

Themenblock 3

Datensicherung / Backup

Wie Sie Ihre Daten schützen und sich so im Schadensfall absichern

Relevanz

Egal wie groß ein Unternehmen ist, Datensicherung ist ein zentraler Bestandteil im Business Continuity Management. Es gibt viele Szenarien, wie Daten verloren gehen können – sei es ein technischer Defekt, ein Cyberangriff, menschliche Fehler oder höhere Gewalt. Wenn Sie Ihre Daten regelmäßig sichern, sorgen Sie dafür, dass eine Datenwiederherstellung immer möglich ist und sichern so den Fortbestand Ihres Unternehmens. Außerdem reduzieren Sie so die Ausfallzeit Ihrer Systeme im Schadensfall und können dadurch enorme Kosten sparen. Im Zuge einer ordnungsgemäßen Datenverarbeitung sind Datensicherungen ohnehin unerlässlich.

Risiken und Gefahren

Der organisatorische Teil der Datensicherung ist mindestens genauso wichtig wie die Datensicherung selbst. Unternehmen sollten klar definieren, wer die Verantwortung für Datensicherung und Datenwiederherstellung trägt und es sollte genügend Zeit für diese Aufgabe eingeräumt werden. Denn eine zu rasche, oberflächliche Bearbeitung kann im Ernstfall viel Zeit und Geld kosten. Scheuen Sie sich nicht, externe Hilfe in Anspruch zu nehmen. Oftmals genügt eine kurze, initiale Beratung, um sich einen Überblick über die verschiedenen Möglichkeiten und Methoden zu verschaffen.

Handlungsempfehlungen

In einer Datensicherung sollten alle Daten enthalten sein, die für die Wiederherstellung eines Systems unerlässlich sind. Dazu gehören u. a. Systemdateien, Software und Anwendungsprogramme, Einstellungen, Benutzerdaten, Dateien und Dokumente, E-Mails und Kontaktdaten, gespeicherte Passwörter und Internetlesezeichen sowie Systeminformationen und Datenbanken.

Ihre Daten können Sie auf verschiedenen Wegen sichern, beispielsweise durch regelmäßiges Anlegen von Backup-Dateien auf externen Datenträgern oder durch das Erstellen von Datenkopien auf Cloud-Diensten wie Google Drive oder OneDrive. Weiterhin sollten die gesicherten Daten verschlüsselt werden, um zu verhindern, dass Dritte sie einsehen oder verändern können.

Vor der Nutzung eines Cloud-Dienstes sollten Sie sicherstellen, dass Ihre Daten und persönlichen Informationen dort sicher und vertraulich behandelt werden. Informieren Sie sich dazu über Datenschutzrichtlinien und Serverstandorte des Cloud-Anbieters. Prüfen Sie ferner, welche Verfügbarkeit die jeweiligen Dienste anbieten.

Wie oft Sie Ihre Daten sichern sollten, kann sehr individuell sein, jedoch mindestens einmal pro Woche ist sinnvoll. Wenn Sie viele Dateien verschieben, erstellen oder bearbeiten, kann eine häufigere Sicherung geboten sein.

Sie können Ihre Daten auch automatisiert sichern lassen – mithilfe von Backup-Programmen. Diese funktionieren in der Regel nach immer demselben Prinzip: Sie erstellen eine Backup-Kopie aller benötigten Dateien und Verzeichnisse an einem bestimmten Ort – bspw. auf einem externen Webserver oder Cloud-Speicher. Dann planen Sie die automatische Erstellung der Sicherungskopie – wie gesagt, möglichst mindestens einmal pro Woche. Ältere Sicherungen werden nach einem vordefinierten Prüfintervall und nur im Falle einer Änderung überschrieben, so dass das Backup immer möglichst synchron zu den lokalen Daten auf Ihrem Rechner ist. Wenn dann eine Systemstörung oder ein Datenverlust auftritt, können Sie die letzte Sicherung verwenden, um das System wiederherzustellen.

Bei der Suche nach einem geeigneten Backup-Programm sind wir Ihnen gern behilflich.

Motiv: Generiert mit der KI Midjourney

Themenblock 4

Sicher im Home Office / Sicher im Netz

Wie Sie Ihr heimisches Büro vor digitalen Angriffen schützen

Relevanz

Home Office und Remote Office sind längst keine Trends mehr, sondern fest etablierte Bausteine in einer modernen Arbeitskultur. Unter dem Stichwort „New Work" arbeiten immer mehr Menschen zu flexiblen Zeiten an dezentralen Arbeitsorten. Eine Herausforderung für die Unternehmenssicherheit! Denn auch Cyberkriminelle versuchen, diesen Umstand zu ihrem Vorteil auszunutzen und auf dem Umweg über persönliche Büros die Sicherheitsstandards von Firmen auszuhebeln. Deshalb ist es wichtig, den Zugriff auf Firmenapplikationen auch aus dem Home Office / Remote Office bestmöglich abzusichern. Welche Möglichkeiten es gibt, lesen Sie hier.

Risiken und Gefahren

Das eigene Zuhause sollte der sicherste Ort der Welt sein – nur häufig ist er es nicht. Insbesondere dann nicht, wenn ihre digitale Welt nicht vor unbefugtem Zugriff geschützt ist. Das beginnt schon beim heimischen Router, der häufig nicht so konfiguriert und gewartet wird, wie der Router in der Firma. Hinzu kommt die Vermischung von privatem und beruflichen Gebrauch des Internets. Gelangt Firmware auf den Router, dringen auch Cyberkriminelle in die Netzwerkverbindung ein. Ein weiteres Risiko ist das in Themenblock 2 beschriebene Social Engineering sowie die geringere Abgrenzung von Berufs- und Privatleben.

So gibt es häufig kein separates Büro, das Laptop steht irgendwo auf dem Wohnzimmertisch, auf dem Bistrotisch oder im Co-Working-Space, Mitbewohner:innen oder Coworker:innen werden Zeuge von Telefonaten und Videocalls. Doch mit ein paar kleinen Maßnahmen lässt sich der Datenschutz im Remote Office – ob zuhause oder an einem anderen Ort – deutlich verbessern.

Handlungsempfehlungen

Selbstverständlich gelten auch am dezentralen Arbeitsplatz die 3 P der IT-Security: Passwörter, Patches und Personen. Darüber hinaus empfehlen wir Ihnen die Umsetzung einiger der folgenden Maßnahmen:

- Trennen Sie berufliche und private Themen, auch räumlich.

Pflegen Sie Ihren privaten Router:

- Regelmäßige Firmware-Updates.
- WLAN-Hauptkennwort und SSID nach Kauf ändern.
- Gäste-WLAN einrichten.

- Nutzen Sie die berufliche Backup-Festplatte nicht für private Dateien.

- Prüfen Sie die Einstellungen Ihrer Smart Home Devices.

- Nutzen Sie VPN für den Zugriff auf das Firmennetzwerk.

- Nutzen Sie Social Media nur mit Bedacht – das Internet vergisst nichts!

- Löschen Sie unnötige Accounts.

- Besuchen Sie nur vertrauenswürdige Webseiten: Orientierung geben das Trusted-Shop-Siegel, Nutzerbewertungen, Google Page Ranks.

- Aktivieren Sie die automatische Browseraktualisierung.

- Installieren Sie nur notwendige Browser-Plugins.

- Speichern Sie Passwörter oder Auto-Fill-Felder wie z. B. für die Kreditkartennummer nicht im Browser - nutzen Sie lieber einen Passwortmanager.

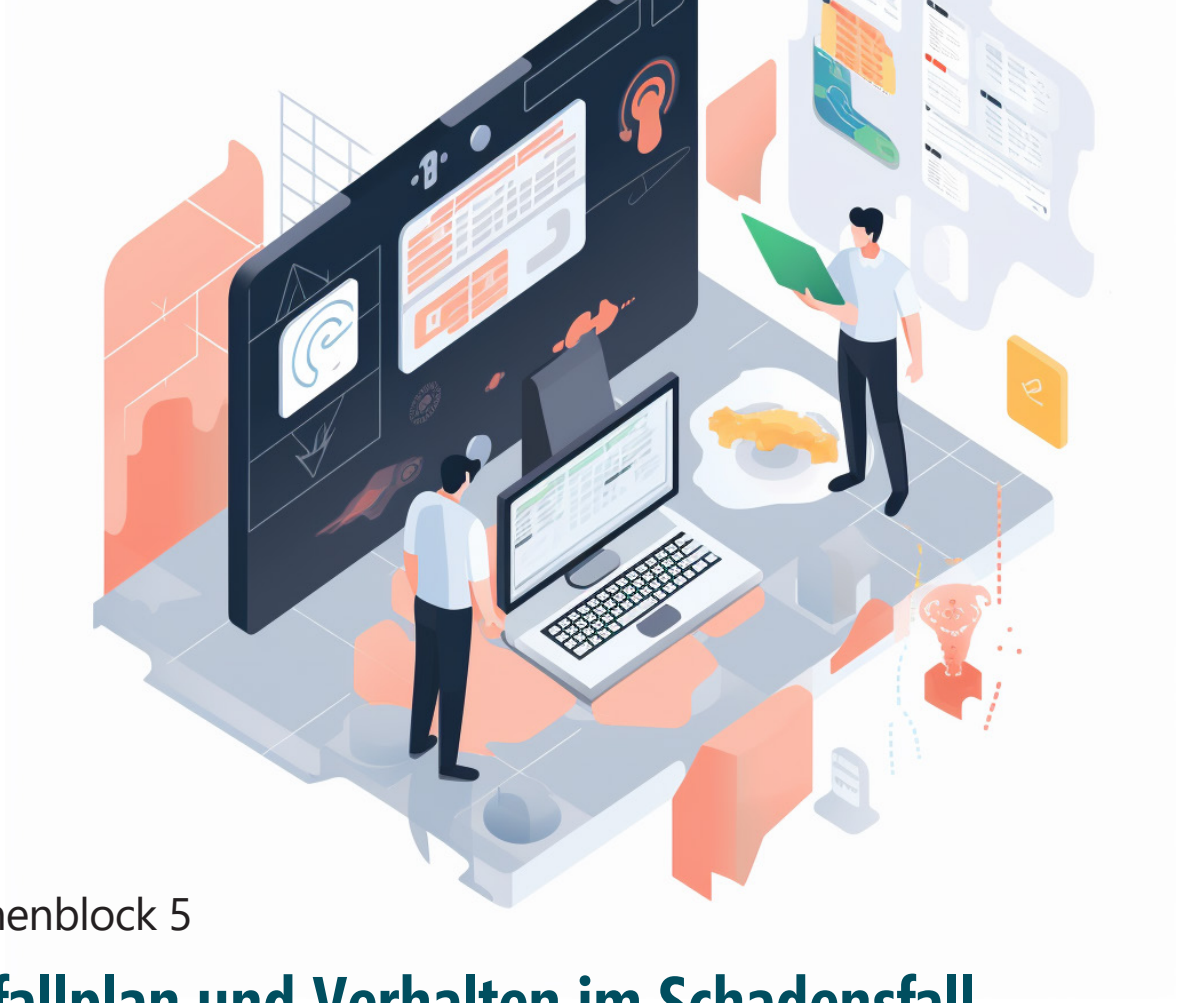
- Aktivieren Sie eine Firewall.

- Installieren Sie eine Antivirensoftware.

- Nutzen Sie Adblocker (z.B. https://ublockorigin.com/de) oder Privacy Badger (https://privacybadger.org/).

- Öffnen Sie keine Links oder Anhänge aus nicht vertrauenswürdigen Quellen https://www.virustotal.com/gui/home/upload).

- Setzen Sie nur die nötigsten Zugriffsberechtigung von Apps auf Ihrem Smartphone.



Motiv: Generiert mit der KI Midjourney

Themenblock 5

Notfallplan und Verhalten im Schadensfall

Über eine gute Vorbereitung und das richtige Verhalten im Ernstfall

Relevanz

Laut BSI gab es im Jahr 2021 in Deutschland 3.356 erfolgreiche Hackerangriffe. Daten aus dem ersten Quartal 2022 liegen noch nicht vor (BSI Lagebericht 2022). Das BSI geht davon aus, dass die Zahlen weiterhin steigen werden. Tagtäglich erhalten Unternehmen Phishing-Mails, ständig werden Sicherheitslücken in Betriebssystemen und Browsern gescannt, permanent wird nach weiteren Einfallstoren gesucht. Von einem Schadensfall sprechen wir, wenn ein Angriff von Cyberkriminellen die Integrität, Verfügbarkeit oder Vertraulichkeit von Daten kompromittiert hat. Dazu zählen Cyberattacken, Schadprogramme, Datenschutzverletzungen, Datenverlust oder unbefugte Zugriffe auf Informationen oder Systeme.

Mittlerweile ist es nicht mehr die Frage, ob ein Unternehmen gehackt wird, sondern wann. Um sich aktiv auf den Schadensfall vorzubereiten und einen Angriff mit möglichst wenig Schaden zu überstehen, sollten Sie einen groben Notfallplan erstellen und von Zeit zu Zeit üben, wie Sie sich im Schadensfall richtig verhalten.

Risiken und Gefahren

Die Erstellung eines Notfallplans ist wichtig, um angemessen auf Schadensfälle reagieren zu können und die Auswirkungen für das Unternehmen so gering wie möglich zu halten. Wer für den Ernstfall gewappnet ist, kann schnell reagieren und Ausfallzeiten kurz halten. Außerdem können Notfallpläne und Notfallübungen die IT-Sicherheit in Ihrem Unternehmen kontinuierlich und nachhaltig steigern. Die Durchführung von Übungen sensibilisiert Ihre Mitarbeitenden und zeigt auf, an welchen Stellen es in Ihrem Unternehmen besonders kritisch werden kann. Sind Sie sich dieser Stellen bewusst, können Sie ganz gezielt Maßnahmen ergreifen, um diese besser zu schützen.

Handlungsempfehlungen

Ein Notfallplan sollte Folgendes beinhalten:

Schritt 1: Alle notfallkritischen Elemente und Prozesse identifizieren und festhalten:

- Welche Daten und Prozesse sind besonders kritisch?
- Welche Geräte nutzen wir?

Schritt 2: Schadensausmaße bewerten:

- Folgen bei Ausfall
- Maximal tolerierbare Ausfalldauer

Schritt 3: Verantwortliche Personen bestimmen:

- Welche Personen sind unverzüglich zu informieren?
- Wer sind die Stellvertreter:innen?

Schritt 4: Sofortmaßnahmen bestimmen:

- Ruhe bewahren
- Beobachten und dokumentieren
- Vorfall melden
- Wenn nötig, Hilfe holen

Schritt 5: Gesetzliche Bestimmungen beachten

- Gibt es Meldepflichten an Aufsichtsbehörden / BSI etc.?

Schritt 6: Wiederanlaufplan

- Zuständigkeiten im Vorfeld klären

Zusammenfassung und Fazit

Vorteile der beschriebenen Maßnahmen

IT-Security ist ein erfolgskritischer Faktor für jedes Unternehmen. Integrität, Verfügbarkeit und Vertraulichkeit sensibler Daten und Systeme sollten deshalb hohe Priorität haben.

IT-Security ist außerdem eine Teamleistung. Wenn das IT-Sicherheitskonzept mit der gebotenen Sorgfalt erarbeitet und von allen Mitarbeitenden getragen wird, sind Sie gut gerüstet. Hier sind regelmäßige Schulungen hilfreich. Und denken Sie daran: Oft können Sie mit kleinen Maßnahmen schon Großes erreichen. Zudem gibt es Stellen, wo sie nützliche und fachkundige Informationen erhalten:

BSI: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Für Wirtschaft, Wissenschaft, Gesellschaft sowie für die Bürgerinnen und Bürger fungiert das BSI als kompetenter Ansprechpartner und Berater zu allen Fragen der Informationssicherheit.

Allianz für Cybersicherheit: Laut der Allianz für Cybersicherheit sind knapp 70 % der Unternehmen und sonstigen Institutionen in Deutschland in den vergangenen zwei Jahren Opfer von Cyberangriffen geworden – Tendenz steigend. Die ACS stellt dazu regelmäßig nützliche Informationen bereit und kümmert sich als Public Private Partnership um eine Verbesserung der IT-Security am Wirtschaftsstandort Deutschland.

Cyber-Sicherheitsnetzwerk: Das Cybersicherheitsnetzwerk ist ein freiwilliger Zusammenschluss von IT-Security-Expert:innen, die effizient und kostengünstig KMU und Bürger:innen bei IT-Sicherheitsvorfällen unterstützen wollen.

Polizei-Zentrale Ansprechstelle Cybercrime: Im Falle eines digitalen Angriffs oder Missbrauchs ist entschlossenes und schnelles Handeln erforderlich. Die zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes stehen Ihnen hier als kompetente Partner zur Verfügung, sowohl für Informationen zur Vermeidung von Cybercrime-Angriffen als auch im Fall von digitalen Straftaten gegen Ihre Firma.

Hessen3C: Mit dem Hessen CyberCompetenceCenter (Hessen3C) hat das Hessische Ministerium des Innern und für Sport eine zentrale Anlaufstelle zum Thema Cybersicherheit in Hessen geschaffen.

RKW Hessen: Das 1921 gegründete Reichskuratorium für Wirtschaftlichkeit in Industrie und Handwerk macht es sich heute zur Aufgabe, Unternehmen bei ihrer digitalen Transformation zu begleiten und zu unterstützen – auch in Fragen der IT-Sicherheit.

EDITH: EDITH ist der European Digital Innovation Hub in Hessen. Er unterstützt kleine und mittlere Unternehmen (KMU), Start-ups und Kommunen kostenlos bei der Umsetzung von Digitalisierungsvorhaben. Neben Künstlicher Intelligenz, High Performance Computing und Advanced Digital Tools liegt eine weitere Kern-Kompetenz von EDITH in der Cybersecurity, insbesondere im Support beim Schutz von Computersystemen, Netzwerken, Daten und anderen digitalen Assets vor Diebstahl-Schäden oder unbefugtem Zugriff durch Cyberangriffe.

ATHENE | Startup Hub für Cybersecurity: Um ATHENE hat sich Deutschlands führende Innovationscommunity für Cybersecurity-Startups gebildet. Sie sind Heimat für alle, die für Innovationen im Bereich Cybersicherheit brennen. Als Hub vernetzen sie Startups, Unternehmen, Investor:innen und Venture Capitalists sowie andere Stakeholder. Wir sind davon überzeugt, dass Innovationen und Gründungen im Bereich Cybersicherheit zu einer sicheren und souveränen Zukunft in Deutschland und Europa beitragen.

"Veranstaltungen wie die vom KDLR mit Micromata begrüßen wir sehr, weil sie das Thema IT-Security noch stärker in die Breite tragen. Die Inhalte helfen uns sehr, unsere rund 50 Mitarbeitenden zu schulen."

Polyas GmbH

Motiv: Generiert mit der KI Midjourney

Informieren Sie sich über die aktuellen Veranstaltungen im KDLR.

jetzt informieren!

Einfach QR-Code scannen.

KDLR
Kompetenzzentrum
für Digitalisierung
im ländlichen Raum

Das Kompetenzzentrum für Digitalisierung im ländlichen Raum ist der Fokus zur Stärkung der Digitalisierung im ländlichen Raum von Hessen.

Impressum

Herausgeber:

House of Digital Transformation e.V.

Mornewegstraße 30

64293 Darmstadt

Pressestelle: +49 6151 –16 752 61

E-Mail: info@hodt-hessen.de

Inernet: www.hodt-hessen.de

Verantwortlich im Sinne des Presserechts:

Hauke Schlüter

Redaktion:

Judith Luther, Tabea Pohlmann und Marco Ziegler (KDLR), Jasmin Macha (House of Digital Transformation), Dominique Wüst und Celina Hartmann (Micromata GmbH)

Grafische Konzeption und Gestaltung:

Gold ‘n‘ Bold

Link zur Publikation: https://hodt-hessen.de/publikationen/

Stand: September 2023

KDLR gefördert durch:

HESSEN
Hessische Staatskanzlei
Hessische Ministerin für
Digitale Strategie und Entwicklung

digitales.hessen

KDLR in Kooperation mit:

IT NETZWERK e.V.
Wir fördern den Vorsprung

REGIONALMANAGEMENT
NORDHESSEN
Gemeinsam.Zukunft.Gestalten.