Praxistipps für die IT-Sicherheit im IT-Alltag

IT-Sicherheits-Fibel

KIEL-IT

Praxistipps für die IT-Sicherheit im IT-Alltag

IT-Sicherheits-Fibel

KIEL-IT

IMPRESSUM

REDAKTION

Bettina Scheider
Manuel Langeheinecke

HERAUSGEBER

Kiel-IT GmbH
Hamburger Chaussee 169

24113 Kiel

TEL.: +49(0) 431 570 85 50-0
FAX: +49 (0)431 / 570 85 50-1
E-MAIL: info@kiel-it.de
WEB: www.kiel-it.de

1. AUFLAGE MAI 2023, 250 STÜCK

BILDNACHWEIS

Cover - Adobe Stock © Tiko
Seite 21 - Adobe Stock © chathuporn

INHALT

PRAXIS-TIPPS FÜR DEN IT-ALLTAG

PRAXIS-TIPPS FÜR DEN IT-ALLTAG

Passwörter

Nutzen Sie grundsätzlich Passwörter! Nur durch Passwörter ist Dritten der Zugang zum PC oder zum Smartphone verwehrt.

Gehen Sie bei der Vergabe Ihrer Passwörter wie folgt vor:

Denken Sie sich ein Passwort aus, das mindestens 3 der nachfolgenden 4 Kategorien enthält:

- Großbuchstaben
- Kleinbuchstaben
- Sonderzeichen
- Ziffern

Vermeiden Sie Passwörter, die durch Dritte leicht zu erraten sind (wie z.B. Vor-und Familiennamen, Geburtstage oder trivial angeordnete Zahlenkombinationen wie 12345678).
Vermeiden Sie außerdem Passwörter, die Sie schon einmal verwendet haben.

TIPP

Denken Sie sich einen Satz mit einem Geschehnis aus Ihrem tatsächlichen Leben aus, der Großschreibung, Sonderzeichen und Zahlen enthält. Nehmen Sie von den Worten dieses Satzes jeweils den ersten Buchstaben.

Beispiel: Der Passwortsatz „Meine Sneaker habe ich 50 % günstiger bekommen“ ergibt das Passwort „MShi50%gb“.

WICHTIG

Verwenden Sie für unterschiedliche Zugänge, z.B. für Windows, Webmaildienste, Internetseiten oder sonstige Anwendungen/Apps, unterschiedliche Passwörter.

Im Internet ist dies eine wichtige Sicherheitsvorkehrung, falls bei einem Internetanbieter, bei dem Sie Kunde sind, Ihr Passwort und Ihre Mailadresse kompromittiert worden sind.

Nur so sind die Logins bei anderen Anbietern davon nicht betroffen, auch wenn Sie dieselbe Mailadresse angegeben haben.

Sichere Verwahrung von Passwörtern

- Passwörter sind stets geheim zu halten!
- Behalten Sie Passwörter am Besten im Kopf!
- Andernfalls ist eine sichere Lösung die Verwendung von verschlüsselten Passworttresoren, wie z.B. dem Netwrix Passwortsafe. Netwrix Passwortsafe eignet sich besonders für das gemeinsame Verwalten von Passwörtern für Teams und kann auf einem eigenen Server installiert werden.
- Passwortlisten in Papierform gehören möglichst in den Tresor.

Nutzung von E-Mail

Prüfen Sie vor dem Versand einer E-Mail,

- dass der Adressat der E-Mail auch der Berechtigte zum Empfang der enthaltenen Information ist.
- dass die Mailadresse des Adressaten richtig ist und Sie bei der Eingabe oder Auswahl nicht versehentlich der Autokorrektur oder einem falschen Vorschlagsfeld auf den Leim gegangen sind.

Versand an mehrere Empfänger

Soll die Mail an eine Vielzahl von Empfängern verschickt werden, ist es wichtig, die Felder CC: (auch „Kopie“) und BCC: (auch „Blindkopie“) korrekt zu verwenden.

Das CC:-Feld ist für Empfänger gedacht, die Kenntnis vom Inhalt haben sollen, ohne selbst aktiv werden zu müssen, und die erfahren sollen, welcher Empfängerkreis die Mail erhalten hat.

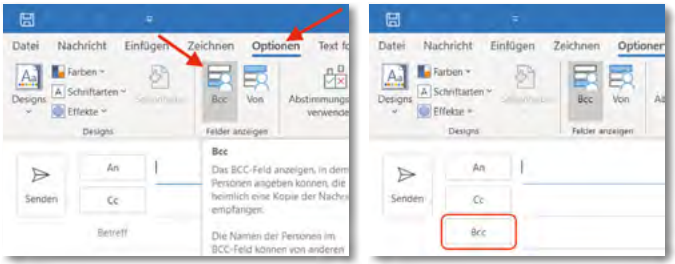
Das BCC:-Feld ist für Empfänger gedacht, für die es keinen Anlass gibt, voneinander zu erfahren, wie z.B. bei Newslettern. Dies ist aus Datenschutzgründen sehr wichtig!

Prüfen Sie zunächst, ob das BCC:-Feld im Adressfeld Ihres Mailprogramms angezeigt wird. Andernfalls richten Sie es dauerhaft ein. Vor dem Versand an mehrere Empfänger ist zu prüfen, ob diese notwendigerweise die Information erhalten müssen.

Einblenden des BCC-Felds in Outlook:

Erstellen Sie eine neue E-Mail. Im nun geöffneten E-Mail-Fenster klicken Sie auf das Menü „Optionen“. Klicken Sie im Anschluss auf das dadurch sichtbare Symbol „BCC“. Nun ist das Feld BCC als weiteres Empfängerfeld unterhalb von „CC“ eingeblendet.

Die Einstellung bleibt für das Erstellen zukünftiger E-Mails erhalten.



Verschlüsselter Versand von Dateianhägen

Wenn Sie Dokumente mit personenbezogenen Daten per E-Mail versenden, sollten diese als verschlüsselter Dateianhang versendet werden.

Bei Office-Dokumenten besteht die Möglichkeit, Dokumente mit einem Kennwortschutz zu versehen.

Unter „Datei/Informationen/Dokument schützen/Mit Kennwort (Passwort) verschlüsseln“ vergeben Sie ein Kennwort.

Teilen Sie dem Empfänger das Kennwort telefonisch oder per SMS mit, auf keinen Fall jedoch durch eine weitere E-Mail!

Anhänge und Links eingehender Mails (Phishing und Social-Engineering)

Besondere Vorsicht ist angesagt, bei allen eingehenden Mails mit Anhängen.

- Haben Sie eine E-Mail von einer Ihnen unbekannten Mailadresse erhalten?
- Oder kennen Sie den Absender, erwarten aber keine E-Mail?

Selbst wenn Sie den Absender kennen und eine Nachricht erwarten:

Öffnen Sie auf keinen Fall ungeprüft den Anhang der Mail oder den in der Mail genannten Link! Prüfen Sie den Link vor dem Klicken, indem Sie mit dem Mauszeiger über dem Link verweilen, OHNE zu klicken. Ihnen wird dann der vollständige Link angezeigt.

Rufen Sie den Absender zunächst an, ob er tatsächlich der Urheber dieser Mail ist.

DENN

durch künstliche Intelligenz oder das sogenannte Social-Engineering ist es für Internetkriminelle möglich, Verbindungen zwischen Personen nachzuvollziehen und dies mit einer gefälschten Mail, die im Anhang oder im Link Schadsoftware enthält, auszunutzen. Dieses Vorgehen ist auch als Phishing bekannt.

Sehr bedenklich sind Anhänge, in den alten Microsoft Office-Formaten, wie .doc, .xls oder .ppt. Wie bereits beschrieben: Öffnen Sie nur Anhänge in den Formaten *.docx, *.xlsx, *.pptx, *.pdf oder *.png!

Und öffnen Sie diese nur, wenn sie von einem sicheren Absender kommen!

Ebenso: Nicht mit einem Kennwort versehene ZIP-Dateien sollten nur geöffnet werden, wenn der Absender bekannt ist und der Versand zuvor angekündigt wurde. Vereinbaren Sie einen Kennwortschutz!

Weitere Informationen zu Phising und Social Engeneering erhalten Sie unter

https://dsgvo-nord.de/whitepaper/wp_ps.pdf

Besteht der Verdacht auf Virenbefall, trennen Sie das Gerät sofort vom Netz/Internet (WLAN-Zugang ausschalten, den Netzwerkstecker ziehen oder den Router ausschalten) und informieren Sie die IT-Betreuung oder Ihren IT-Dienstleister.

BEACHTEN SIE IN DIESEM FALL DIE HINWEISE AUF DER RÜCKSEITE DIESER FIBEL!

Speicherung von Dokumenten

Achten Sie darauf, dass Microsoft Office-Dokumente immer in den 2007 eingeführten Formaten (*.docx, *.xlsx oder *.pptx) gespeichert werden. Dies erledigen Sie über den Menüpunkt „Speichern unter“ und die Auswahl des richtigen Formats im Feld „Dateiformat“.

Auf diese Weise ist es Ihnen auch möglich, von Ihnen verwendete Dateien, die noch im alten Format abgespeichert waren (*.doc, *.xls, *.ppt), unter dem neuen Format abzuspeichern.

Dies ist wichtig, wenn Sie diese Dateien per E-Mail versenden wollen. Denn: Befinden sich alte Dateiformate im Anhang einer Mail, werden diese i.d.R. aus Sicherheitsgründen von Spamfiltern, Mail-servern oder Firewalls gelöscht, so dass Ihre E-Mail ohne einen Dateianhang beim Empfänger ankommt oder vollständig ohne Rückmeldung gelöscht wird.

Umgekehrt ist es so, dass Sie kein fremdes Dokument im *.doc, *.xls, *.ppt Format öffnen sollten, da darin Schadsoftware versteckt sein kann!

Mobile Datenträger verschlüsseln

Bei USB-Sticks, externen Festplatten, Notebooks, Smartphones oder Tablets muss die Datenträgerverschlüsselung aktiviert sein, um bei Verlust des Gerätes einer Datenpanne vorzubeugen.

Smartphones, Tablets und Notebooks bieten häufig eine integrierte, jedoch i.d.R. nicht ab Werk aktivierte Datenträgerverschlüsselung an.

Fragen Sie Ihren IT-Administrator, wie eine Datenträgerverschlüsselung für mobile Endgeräte mit einem Android oder Windows-Betriebssystem aktiviert werden kann. Die Datenträgerverschlüsselung ist bei Geräten der Firma Apple bereits ab Werk aktiviert.

Zum Verschlüsseln von USB-Sticks können Sie das kostenlose Open-Source Tool „Veracrypt" verwenden. (https://veracrypt.fr).

Mit einer Windows Pro-Edition können Sie mittels integriertem Tool „Bitlocker To Go" Wechseldatenträger verschlüsseln.

Clean-Desk-Policy („Grundsatz des sauberen Schreibtischs")

Sichern Sie Ihren Arbeitsplatz und Homeoffice immer vor Einsichtnahme oder dem Zugang Dritter zu personenbezogenen Daten:

- Achten Sie darauf, dass auf Ihrem Schreibtisch und Ihrem PC-Bildschirm nur Akten offen bzw. Dateien sichtbar sind, die Sie aktuell für die Bearbeitung benötigen.
- Handelt es sich dabei um Dokumente mit personenbezogenen Daten, sollte davon keine andere Person Kenntnis nehmen können.
- Wenn Sie Ihren Arbeitsplatz verlassen oder wenn Besucher den Raum betreten, schließen Sie alle offenen Akten und sperren Sie Ihren PC-Bildschirm, bzw. positionieren Sie die Person so, dass sie keine Einsicht nehmen kann.
- Überprüfen Sie Ihren Schreibtisch daraufhin, ob interessante schriftliche Notizen lesbar sind (Post-it® Haftnotizen, beschriebene Schreibunterlage usw.), die Sie besser vor der Kenntnisnahme Dritter schützen sollten.

Verlassen des Arbeitsplatzes

Aktivieren Sie beim Verlassen Ihres Windows-PCs oder Laptops die Desktopsperre mit dem Tastenkürzel  + L

Am Mac drücken Sie **[ctrl] + [cmd] + [Q]**
oder indem Sie **[ctrl]** und den **Touch-ID-Sensor**
gleichzeitig drücken.

Fahren Sie am Arbeitsende Ihren PC herunter. Räumen Sie Ihren Schreibtisch auf und offenliegende Akten weg. Schließen Sie Fenster und Türen.

Telefon

Bevor Sie am Telefon Auskünfte geben, vergewissern Sie sich, dass die Person am Telefon auch wirklich diejenige Person ist, für die sie sich ausgibt.

Sollten Sie Zweifel an der Identität der Person haben, verschicken Sie die gewünschte Information per Post an die in der Verwaltung hinterlegte Anschrift oder Mailadresse.

Nehmen Sie in diesem Fall keine neue Anschrift oder Mailadresse zum Versand der Informationen entgegen, dies könnte ein Trick sein.

Senken Sie die Lautstärke beim Telefonieren, wenn sich Besucher in Ihrer Nähe befinden.

Besucher, Reinigungspersonal oder Handwerker

Wenn Sie einen Besucher im Büro empfangen, achten Sie darauf, Telefonate und Akten vor dem Besucher geheim zu halten und ihn in den Räumen nicht allein zu lassen.

Computer-Fernwartung

Bevor Sie einem Service-Techniker den Zugriff auf Ihren Computer per Fernwartung erlauben, vergewissern Sie sich, dass die Person tatsächlich dazu berechtigt ist.

Bevor Sie die Zugriffserlaubnis erteilen, schließen Sie alle für den Service-Techniker nicht relevanten Programme. Bleiben Sie während der gesamten Fernwartung am PC.

Falls eine Beaufsichtigung nicht möglich ist, aktivieren Sie eine Sitzungsaufzeichnung als Beweissicherung, im besten Fall ist eine regelmäßige Sitzungsaufzeichnung der Service-Techniker vertraglich vereinbart.

Virenschutz

Stellen Sie sicher, dass der Virenschutz auf dem PC eingeschaltet und aktuell ist.

Installieren Sie Software-Updates zeitnah oder wenden Sie sich an Ihren IT-Administrator oder IT-Dienstleister.

Versichern Sie sich regelmäßig bei Ihrem IT-Administrator oder IT-Dienstleister, dass die Funktionstüchtigkeit der Sicherheitssysteme regelmäßig überprüft bzw. aktualisiert wird (z.B. durch eine Firewall).

Datensicherung digital und analog

Legen Sie alle personenbezogenen Dateien im Verwaltungsprogramm oder in Dateiordnern ab, von denen Sie wissen, dass sie durch eine Datensicherung regelmäßig gesichert werden.

Aktenordner mit vertraulichen personenbezogenen Informationen, wie zum Beispiel Personalordner, sind in verschlossenen Schränken zu verwahren.

Zutritt zum Serverraum

Zutritt zu Serverräumen ist nur berechtigten Personen gestattet. Die Zutrittstür zum Serverraum muss auch tagsüber immer verschlossen sein.

Personen, die den Serverraum zum Wechsel der Datensicherungsmedien betreten, müssen dafür sorgen, dass sie den Raum im Anschluss wieder verschließen!

Serverräume sind ausschließlich zur Verwahrung von aktiv verwendeten IT-Komponenten gedacht.

Ausgediente Geräte erhöhen die Brandlast und gehören nicht in den Serverraum.
Ein Serverraum ist kein Lager, Aktenarchiv oder Abstellraum.

Planmäßige Vernichtung von Datenspeichern und Aktenordnern

Stellen Sie sicher, dass Datenträger und Aktenordner von einer Spezialfirma unwiederbringlich und datenschutzkonform vernichtet werden.

Wird ein Drucker oder ein Kopierer ausgetauscht, achten Sie darauf, dass Ihnen die Festplatte ausgehändigt wird. Alternativ sollte eine unwiederbringliche Löschung der Daten vertraglich vereinbart sein.

Benutzen Sie für Papierunterlagen mit personenbezogenen Daten einen Aktenschredder.

Unterlagen, die personenbezogene Daten enthalten, müssen mindestens unter Sicherheitsstufe 4 (z. B. Personaldaten, Bewerbungsunterlagen) bzw. Sicherheitsstufe 5 (z. B. Gesundheitsdaten) vernichtet werden.

Messengerdienste, WhatsApp, Miterarbeiter-Apps

Darf WhatsApp aufs Diensthandy?

Die Antwort lautet eindeutig: Nein.

Der Dienst ist mit weiteren Social-Media-Diensten wie Facebook und Instagram verbunden und für die Weitergabe der auf dem Handy befindlichen Daten bekannt (Adressbuch, Fotos, ggf. andere Informationen).

Interessant sind hier vor allem die sogenannten Meta-Daten, also zu welcher Uhrzeit Sie mit wem in welcher Häufigkeit und an welchen Orten kommunizieren, und nicht die Texte und Bilder im Chat-Verlauf selbst.

Erteilen Sie WhatsApp bei der privaten Nutzung niemals die Standort- oder Mikrofonfreigabe.

Auf Instant Messenger müssen Sie dennoch nicht verzichten: Mit den Diensten Signal (kostenlos) und Threema.ch gibt es datenschutzkonforme Alternativen.

Die Verbreitung von WhatsApp im privaten Umfeld ist sehr hoch, lassen Sie sich davon jedoch nicht entmutigen, die Installation eines alternativen Messengers vorzuschlagen oder durchzusetzen.

In kleineren Gruppen ist die gemeinsame Installation einer neuen App meist in wenigen Minuten erledigt.

Mittlerweile etablieren sich umfangreichere Mitarbeiter-Apps wie Quiply, mit denen ein sicherer Austausch gewährleistet ist. Sie bieten darüber hinaus weitere Team-Funktionen wie Channels, Mitarbeiterverzeichnisse, Push-Nachrichten "an Alle" in Echtzeit, Umfragen, Abwesenheitsregelungen, Intranet-Dokumente (z.B. Anweisungen, Richtlinien, Verfahren) und Quick-Links zu weiteren Unternehmensanwendungen.

Alternativen zu Doodle

Die Online-Terminplanung mit Doodle ist sehr beliebt. Aber Doodle verfügt über keinen effektiven Zugriffsschutz und verkauft die Daten ihrer Benutzer (IP-Adresse, Tracking) regelmäßig an über 1000 Werbepartner in Echtzeit.

Verwenden Sie als Alternative datenschutzkonforme Dienste, wie den DFN Terminplan 4 des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. :

- **https://terminplaner4.dfn.de**
- **https://nuudel.de**

Alternativen zur Google-Suchmaschine

Anonym suchen und trotzdem alles finden:

- **https://www.startpage.com und**
- **https://duckduckgo.com**

Diese Alternativen nutzen die Suchmaschine Google, ohne dass der Internetkonzern Sie tracken kann. Dabei sammeln und teilen diese Anbieter keinerlei persönliche Informationen!

Schutz der Privatsphäre durch Browser

Die Internet-Browser von Firefox, Safari und Brave setzen von sich aus auf Datensparsamkeit und verhindern durch Voreinstellungen, dass der Nutzer beim Surfen eine Datenspur hinterlässt (nähere Informationen bei den Anbietern).

Umgang mit Cookies

Internetseiten benötigen für eine korrekte Seitendarstellung Informationen zu Betriebssystem, Monitor u.a.m. Ihres Rechners. Die dafür gesetzten Dateien (technische Cookies) sind deshalb notwendig für die Anzeige der Webseite.

Gleichzeitig wollen die Webseitenbetreiber auch viele andere Cookies setzen, um Informationen zu Ihrem Surf-Verhalten zu sammeln und auszuwerten, für ein Profiling, das Schalten individualisierter Werbung und den Verkauf Ihrer Daten an Dritte in Echtzeit. Die Webseitenbetreiber holen sich im günstigsten Fall Ihre Einwilligung über „Cookie-Banner" (Consent-Banner).

Mit dem Anklicken des meist farblich leuchtenden Buttons „Speichern" oder „Cookies akzeptieren" erlauben Sie dort das Setzen aller Cookies und die Einbindung weiterer externer Dienste. Nicht selten werden dann bis zu 1200 Partner in Echtzeit über Ihr Surf-Verhalten informiert, dies passiert z.B. bei eBay-Kleinanzeigen, wenn Sie Cookies nicht ablehnen.

Wenn Sie dieses Sammeln Ihrer Daten nicht erlauben wollen, lesen Sie die Angaben des Cookie-Banners bitte genau und klicken Sie auf den eher unscheinbar gehaltenen Link wie „Alle Ablehnen", „Einstellungen speichern", „nur technische Cookies".

Werden Sie gezwungen, die Auswahl eine Ebene tiefer zu treffen (z.B. unter „weitere Einstellungen"), achten Sie darauf, auch unter dem Reiter „berechtigtes Interesse" alle Auswahlmöglichkeiten auf „Aus" zu stellen.

Datenpannen, Datenklau oder Datenverlust

Eine Datenpanne liegt vor, wenn Daten (digital oder in Papierform) verloren gehen, entwendet oder unbefugten Personen zugänglich gemacht wurden.

BEISPIELE

- Versand eines Faxes oder einer E-Mail an den falschen Adressaten
- Newsletterversand an E-Mail-Empfänger unter CC anstatt BCC
- Verlust eines USB-Sticks mit personenbezogenen Daten
- Diebstahl von Unterlagen bei einem Einbruch
- Ein Hackerangriff auf die Webseite oder das IT-System

Halten Sie sich an den in Ihrer Organisation vorgesehenen Ablauf zur Meldung einer Datenpanne:

Informieren Sie unverzüglich den Datenschutzkoordinator oder den Verantwortlichen für den Datenschutz. Diese werden weitere Stellen wie die IT-Abteilung, den Datenschutzbeauftragten und die Aufsichtsbehörde informieren.

Dokumentieren Sie sofort den Hergang und machen Sie eine Bestandsaufnahme.

Benutzen Sie das Datenpannen-Meldeformular der zuständigen Datenschutz-Aufsichtsbehörde. In bestimmten Fällen müssen auch die Betroffenen selbst informiert werden.

Homeoffice

Was muss im Umgang mit personenbezogenen Daten im Homeoffice beachtet werden?

Für die Einrichtung des Arbeitsplatzes zu Hause ist es wichtig, dass Sie ungestört arbeiten können und dass Dritte keinen Einblick und keine Einsicht erhalten.

Werden Dokumente und IT-Geräte vom Arbeitsplatz mit nach Hause genommen?

Achten Sie dabei darauf, dass:

- Ihr Laptop oder PC mit einem sicheren Passwort geschützt ist,
- die Festplatte und auch andere externe Speichermedien verschlüsselt sind,
- Papierdokumente in abschließbaren Schränken oder Schubladen aufbewahrt werden,
- vertrauliche Telefonate vertraulich bleiben, d.h. weder Familienmitglieder, Nachbarn noch andere Personen das Gespräch mitverfolgen können,
- Sie Ihre Sachen grundsätzlich nicht unbeaufsichtigt lassen,
- beim Verlassen des Platzes der Bildschirm mit Passwort gesperrt oder das Gerät ausgeschaltet ist
- Daten über eine verschlüsselte VPN-Verbindung abgelegt werden.

Bedenken Sie dies ebenfalls, wenn Besucher, Handwerker oder Reinigungskräfte Ihr Homeoffice betreten.

Backup/Datensicherung

Ein Backup bzw. eine Datensicherung hilft nach einem Ernstfall bei der Wiederherstellung des Datenbestandes, wenn dieser z.B. durch einen Virus, einen Festplattendefekt oder durch Diebstahl geschädigt wurde.

Wie gelangt man wieder an seine Daten?

Durch eine regelmäßige Sicherung von System und Dateien können die Daten schnell wiederhergestellt werden. In einigen Betriebssystemen wird zur Datensicherung ein Tool eingesetzt, dass die Datensicherung auf allen angeschlossenen Geräten sicherstellt.

WICHTIG

- Darauf achten, dass die Datenträger, auf denen die Daten gesichert werden (externe Festplatte, NAS, USB-Stick), verschlüsselt sind,
- In regelmäßigen Zeitabständen sichern, wie täglich, wöchentlich etc.
- Im Wechsel auf mehreren Datenträgern sichern und die Datensicherungen an einem sicheren Ort verwahren,
- Eine Prüfung vornehmen, ob die Datenwiederherstellung auch gelingt.

Welche Tools können helfen:

Die Betriebssysteme enthalten Anwendungen für die Datensicherung: „Systemabbild erstellen“ (Windows) und „Time Machine“ (Mac-OS).

TIPPS

Backup

DIE BESTEN BACKUP-LÖSUNGEN FÜR KMU

Professionelles "Backup-as-a-Service" für Ihr Unternehmen.

Daten sind heute eine kritische Ressource jedes Unternehmens. Sowohl Ihre, als auch die Daten Ihrer Kunden, sollten stets verfügbar und immer umfangreich geschützt sein.

https://kiel-it.de/aktuelles/die-besten-backup-losungen-fur-kmu

Prävention

IHR WEG ZUR HUMAN FIREWALL

IT-Sicherheit ist heute wichtiger denn je. Täglich kommen fast 400.000 neue Schadsoftware Varianten auf den Markt. Die Angreifer entwickeln neue Methoden, um technische Barrieren wie Firewalls und Virenscanner zu umgehen.

Ihr Ziel ist der Mensch vor dem PC.
Er ist die größte Gefahr für Ihre IT-Sicherheit.
Deshalb ist eine Sensibilisierung Ihrer Mitarbeiter das A und O.

https://kiel-it.de/aktuelles/ihr-weg-zur-human-firewall

KIEL-IT

Wer
meldet?

Welches
IT-System ist betroffen?

Wie
haben Sie mit dem IT-System gearbeitet?

Ruhe bewahren und IT-Notfallnummer anrufen

IT-Notfall?

0431 / 570 85 50-0

- Arbeit am IT-System einstellen
- Internetverbindung trennen
- Beobachtungen dokumentieren
- auf Anweisungen warten

Was
haben Sie beobachtet?

Wann
ist das Ereigniss eingetreten?

Wo
befindet sich das betroffene IT-System? (Gebäude Raum, Arbeitsplatz)