Date: 06.05.2024

Freiburger Nachrichten

Freiburger Nachrichten
1701 Freiburg
026/ 505 34 34
https://www.freiburger-nachrichten.ch/

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 16'195
Parution: 5x/semaine

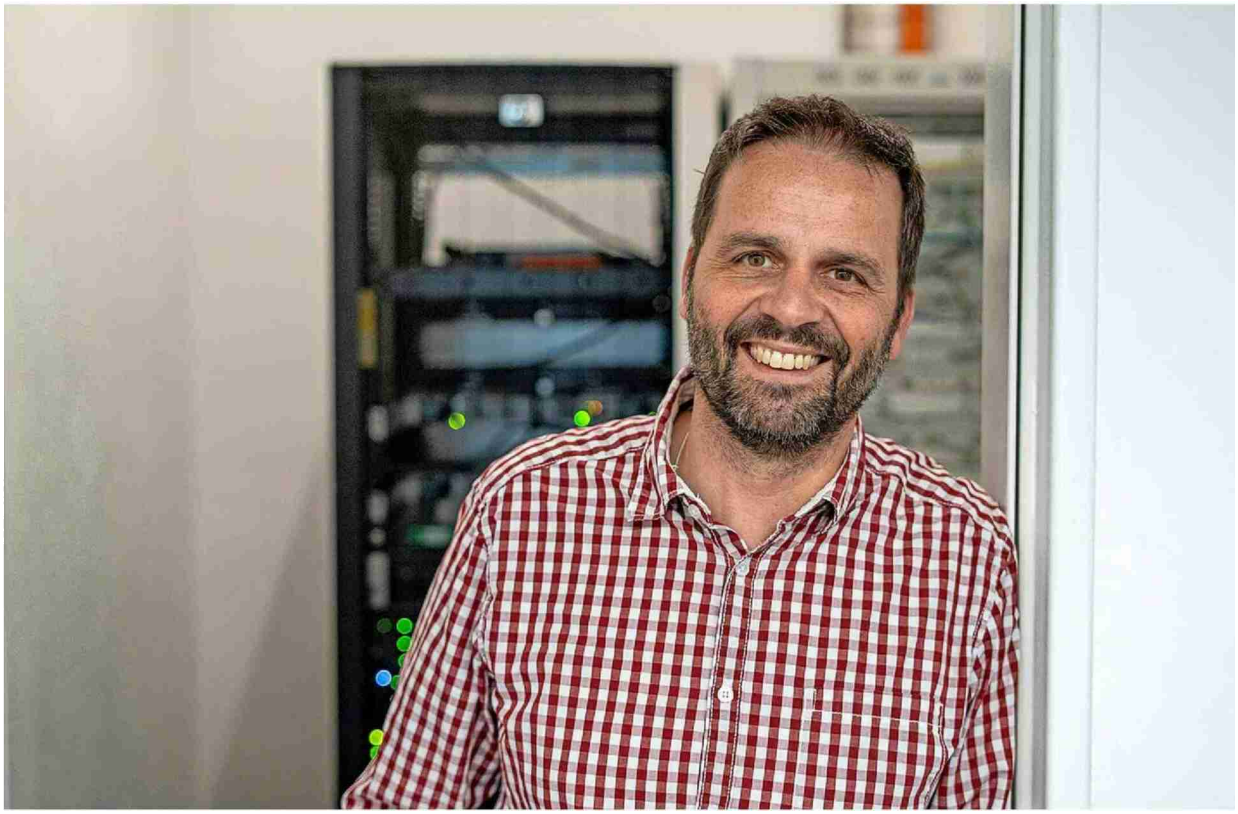
Page: 3
Surface: 102'868 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91831292
Coupure Page: 1/3

Sicher im Netz unterwegs: Das ändert sich durch künstliche Intelligenz

Im Rahmen des Cybersecurity-Seminars der Hochschule für Technik und Architektur Freiburg finden im Mai auch Workshops für die Allgemeinheit statt. Cybersecurity-Experte Michael Mäder gibt Auskunft, wie man sicher im Internet unterwegs ist.



IT-Experte Michael Mäder ist Teil des Organisationsteams der Cybersecurity-Seminare in Freiburg. Bild: Livio Baeriswyl

Martina Schmid

Freiburg Ein nigerianischer Prinz bietet in gebrochenem Englisch eine Millionensumme, dafür möchte er Hilfe dabei, sein Vermögen aus dem Land zu schmuggeln: Diese Spam-Nachricht ist bei allen, die im Besitz einer E-Mail-Adresse sind, schon einmal in dieser oder ähnlicher Form im Postfach gelandet. Inzwischen gehen die Betrügerinnen und Betrüger jedoch, unterstützt durch künstliche Intelligenz (KI), viel gewiefter vor. IT-Experte Michael Mäder erklärt im Gespräch, was die Chancen und die Gefahren der neuesten Entwicklungen sind und wie man sich als Privatperson schützen kann.

Michael Mäder, finden Sie, dass Menschen zu sorglos mit ihren Daten umgehen?

Ich höre oft von Leuten, dass es bei ihnen ja sowieso nichts zu holen gibt, sie wären nicht interessant für Hacker. Aber das stimmt nicht. Privatpersonen können ein Sprungbrett sein, beispielsweise zur Firma, wo sie arbeiten. Wenn jemand das gleiche Passwort für den Facebook-Account und den Arbeitscomputer verwendet, kann das gefährlich werden, wenn bei einem Angriff auf Facebook das Passwort gestohlen wird. Mithilfe dieses Passworts können Hacker dann ins Netzwerk des Unternehmens gelangen und sich so Zugriff verschaffen zu internen Daten, zur Website, zu E-Mails und so weiter.

Es gibt kaum Leute, die nicht mindestens ein Konto in den sozialen Medien haben. Wo liegen dort die Gefahren?

Man sollte gut aufpassen, was man preisgibt. Im Cyberraum habe ich oft das Gefühl, dass das Verlangen nach Likes stärker ist als die Überlegung, ob diese persönlichen Informationen wirklich für jedermann einsehbar sein müssen. Das klingt jetzt vielleicht etwas paranoid, aber je mehr man im Internet preis-

Date: 06.05.2024

Freiburger Nachrichten

Freiburger Nachrichten
1701 Freiburg
026/ 505 34 34
https://www.freiburger-nachrichten.ch/

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 16'195
Parution: 5x/semaine

Page: 3
Surface: 102'868 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91831292
Coupure Page: 2/3

«Inzwischen können Betrügerinnen und Betrüger fehlerfreie, perfekte Texte verfassen lassen.»

gibt, desto präziser können Hacker Cyberattacken gestalten. Statt «dein Paket steckt beim Zoll fest, überweise uns Geld», wirst du dann mit Vornamen angesprochen und an den Mitgliederbeitrag deines echten Fussballclubs erinnert. Die veröffentlichten Daten können aber auch reale Konsequenzen haben: Einbrecher wählen meistens nicht einfach ein zufälliges Haus, sondern suchen sich gezielt eines aus. Zum Beispiel, wenn sie in den sozialen Medien sehen, dass die Besitzerinnen oder Besitzer gerade auf den Seychellen in den Ferien sind.

Welche Rolle spielt künstliche Intelligenz, die KI, dabei?

Die meisten wissen: Wenn sich in einer E-Mail-Nachricht Schreibfehler befinden oder die Grammatik nicht stimmt, handelt es sich vermutlich um Phishing. Das sind gefälschte E-Mails, die einen dazu animieren, auf einen Link zu klicken und dann Informationen preiszugeben. Nun kommt aber KI ins Spiel. Inzwischen können Betrügerinnen und Betrüger fehlerfreie, perfekte Texte verfassen lassen. Je mehr in einer E-Mail-Nachricht stimmt und Sinn macht, desto weniger überlegen die Leute, ob es sich eventuell um eine gefälschte Nachricht handelt. Wenn diese dann vom «richtigen» CEO der Firma stammt, der oder die um eine dringende Überweisung bittet, wird es gefährlich.

Wenn ich ein neues Passwort erstelle, wird nach Zahlen, Zeichen, Gross- und Kleinschreibung verlangt. Ist das nötig?

Es gibt eine berühmte Liste, auf der geleakte Passwörter gesammelt werden. Auf ihr sind inzwischen über 14 Millionen Passwörter zu finden. Bei einer «Dictionary Attacke» probiert ein Programm systematisch alle Optionen durch. Wenn mein Passwort sich auf einer solchen Liste befindet oder aus einem normalen Wort besteht, kann das Programm es in Sekundenschnelle knacken. Die Hardware wird immer besser und kann inzwischen viele Versuche parallel laufen lassen. Deshalb ist es gut, ein möglichst kompliziertes Passwort zu haben. Wichtig ist auch: Auf keinen Fall für alles das gleiche Passwort nutzen, sondern für jeden einzelnen Service ein eigenes.

Wie soll man sich das alles merken?

Die beste Lösung dafür ist ein Passwortmanager, ein kleines Programm auf dem PC oder dem Handy. Dieser Manager enthält alle Passwörter, die schliesslich mit einem Masterpasswort geschützt sind. Beim Gebrauch eines solchen Managers weiss man, dass die Passwörter bei der Eingabe sicher verschlüsselt werden. Die vorinstallierten Programme für die Passwortverwaltung auf dem Computer und dem Handy sind ebenfalls in Ordnung – auf jeden Fall besser, als das gleiche Passwort mehrmals zu verwenden oder es auf einem Zettel oder in

«Über die Hälfte aller weltweiten Hacks passieren über Phishing.»

einem ungeschützten Dokument zu notieren.

Wieso ist es unsicher, das Passwort auf einem Notizzettel zu notieren? Den kann niemand hacken.

Es reicht, dass man beispielsweise in den sozialen Medien ein Foto veröffentlicht, auf dem der Zettel zu sehen ist. Oder dass man den Laptop, an dem ein Passwort auf einem Post-it befestigt ist, im Zug benutzt und der Nachbar freie Sicht auf das Passwort hat.

Inzwischen sind immer mehr Geräte miteinander vernetzt. Wie wahrscheinlich ist es, dass meine Zahnbürste gehackt wird oder mein Elektroauto selbstständig einen Unfall verursacht?

Diese Szenarien sind momentan noch nicht sehr realistisch, aber möglich. Jedes Gerät, das verbunden ist, ist ein kleiner Computer. Oft sind diese vom Internet her zugänglich. Das kann gefährlich werden, wenn das Gerät nicht korrekt konfiguriert ist oder Schwachstellen aufweist. In diesem Fall könnte das Gerät missbraucht werden, um zum Beispiel in einer «Distributed Denial-of-Service-Attacke» mitzumachen. Dabei werden viele vernetzte, gehackte Geräte zu einem Bot-Netz zusammengeschlossen, das dann ganz viele Anfragen an eine Website stellt, bis diese unter der zu grossen Last zusammenbricht. Das könnte einerseits als Machtdemonstration genutzt werden, wenn es sich um Angriffe auf eine öffentliche Website handelt, oder zur Erpressung, beispielsweise bei einem Onlineshop. Es ist also sehr wichtig zu verstehen, dass alle verbundenen Geräte, man spricht hier auch von IoT, Internet of Things, ebenfalls einen minimalen Schutz benötigen.

In den Ferien im Ausland sind viele auf öffentliche WLAN-Netze angewiesen. Was müssen Reisende hier beachten?

In einem öffentlichen Netzwerk sind die Daten zwischen dem Computer oder dem Handy und dem Accesspoint, zum Beispiel dem Router, unverschlüsselt. Theoretisch können also alle mithören. Nun ist es so, dass die meisten Applikationen und Websites die Daten auf dem Gerät verschlüsseln und erst dann hinausschicken. Aber auch hier ist man sich nie sicher, was genau im Hintergrund passiert. Daher sollten solche öffentlichen, nicht geschützten Accesspoints lieber nicht gebraucht werden. Vor allem, wenn man schützenswerte Daten eingeben oder austauschen möchte. Da ist es besser, wenn man den Computer mit dem eigenen Handy verbindet und so ins Internet geht.

Haben Sie noch weitere Tipps, wie man im Internet sicher unterwegs ist?

Der wichtigste Faktor ist immer der Mensch. Über die Hälfte aller weltweiten Hacks passieren über Phishing. Man sollte ein gesundes Misstrauen haben und vor dem Klicken kurz überlegen, ob das Gelesene Sinn macht. Wenn etwas unerwartet oder überraschend kommt, besser schnell nachfragen oder die E-

Date: 06.05.2024

Freiburger Nachrichten

Freiburger Nachrichten
1701 Freiburg
026/ 505 34 34
https://www.freiburger-nachrichten.ch/

Genre de média: Médias imprimés
Type de média: Presse journ./hebd.
Tirage: 16'195
Parution: 5x/semaine

Hes·so

Page: 3
Surface: 102'868 mm²

Ordre: 1073023
N° de thème: 375.009

Référence: 91831292
Coupure Page: 3/3

Mail ignorieren. Von technischer Seite her sollte man regelmässig Updates einspielen, nicht nur auf dem PC, sondern auch auf dem Smartphone. Backups lohnen sich auch, man sollte keine Daten ausschliesslich auf der Festplatte haben. Wenn man die Daten in einer Cloud speichert, ist eine Zwei-Faktor-Authentifizierung sinnvoll. Die ist zwar in der Anwendung etwas umständlich, aber erhöht die Sicherheit enorm.

Spezialisiert in Cybersecurity

Michael Mäder ist seit vier Jahren assoziierter Professor an der Hochschule für Technik und Architektur, wo er unter anderem Vorlesungen im Bereich Informatik- und Kommunikationssysteme sowie Cybersecurity hält. Im Institut für sichere und intelligente Systeme der Hochschule für Technik und Architektur Freiburg leitet und arbeitet er in Projekten im Bereich Cybersecurity mit. Zuvor war er dreizehn Jahre lang bei der Swisscom in verschiedenen Bereichen als Sicherheitsexperte tätig. Er hat einen Masterabschluss in Computer- und Netzwerkwissenschaften der ETH Lausanne. *(mes)*

Cybersecurity-Seminare in Freiburg

Anlass Am 23. Mai findet in Freiburg das Cybersecurity-Seminar zum Thema «Von digitalen Spuren bis hin zu Cyber-Ermittlungen der Justiz» statt. Die Präsentationen halten Vertreter der Kantons- und der Bundespolizei. «Zusätzlich bieten wir dieses Jahr Sicherheitsworkshops zu den Themen E-Banking und zum elektronischen Patientendossier», so Michael Mäder. Diese können auf Deutsch oder Französisch besucht werden. Eine Anmeldung ist nötig.

Hinter dem «Freiburg Cybersecurity Seminar» stecken mehrere Professoren sowie aktuelle und ehemalige Studierende der Hochschule für Technik und Architektur. «Das Ziel ist, in Freiburg eine Cybersecurity-Community zum Leben zu erwecken», erklärt Mäder. Die Idee entstand schon vor vielen Jahren, schlief aber mehrmals wieder ein, bis eine Gruppe sie vor zwei Jahren reaktivierte. *(mes)*

Weitere Informationen unter *www.fr-cybersecurity.ch*