Transkript Folge 43
Cybersecurity: PSA für den PC

Torin Zander
Fakt ist, dass quasi alle Unternehmen permanent angegriffen werden, muss man sagen. Sei es durch E-Mails, sei es durch wirklich Versuche, Schwachstellen zu finden, sei es aber auch durch physische Versuche in ein Unternehmen einzudringen, dort Netze zu kompromittieren. Auch das passiert.

Intro
Ganz sicher. Der Podcast für Menschen mit Verantwortung.

Katrin Degenhardt
Ganz sicher, so heißt der Podcast der BG ETEM. Und der Name ist hier Programm. Wir wollen, dass Menschen sicher sind. Bei der Arbeit und auch auf dem Arbeitsweg. Wie das gelingt, was Unternehmen tun, damit ihre Leute gesund bleiben, Herausforderungen und Lösungen im Arbeitsschutz, darüber spreche ich mit meinen Gästen. Das sind Expertinnen und Experten, Unternehmerinnen und Unternehmer, Sicherheitsfachleute und Beschäftigte aus Mitgliedsbetrieben der BG ETEM.
Und die erzählen mir hier, was sie bewegt. Ich bin Katrin Degenhardt, Moderatorin und Gastgeberin. Und jetzt geht's los.

Heute sprechen wir über das Thema Cybersecurity oder auch Cybersicherheit. Es geht also um den Schutz von Computersystemen, Netzwerken, Programmen und Daten vor digitalen Angriffen. Diese Angriffe können von Akteuren ausgehen, die versuchen, unautorisierten Zugang zu sensiblen Informationen zu erlangen, oder den Betrieb von Systemen zu stören. Der Begriff Cybersicherheit umfasst eine Vielzahl von Technologien, Prozessen und Maßnahmen, die dazu dienen, Bedrohungen zu erkennen, abzuwehren und Schäden zu minimieren.
Klingt das komplex? Ja, das ist auch komplex. Aber Arbeitsschutzverantwortliche müssen sich damit auseinandersetzen, denn in einer durchdigitalisierten Arbeitswelt trägt Cybersicherheit auch zur Arbeitssicherheit bei.
Sie sollten Risiken kennen, passende Schutzmaßnahmen zu ergreifen und Beschäftigte immer wieder zu sensibilisieren. Unser Gast kann das Thema einerseits gut erklären und hat andererseits auch ein paar gute Tipps im Gepäck. Torin Zander kümmert sich in der IT-Abteilung der BG ETEM federführend um das Thema Cybersicherheit. Und jetzt ist er hier bei mir. Herzlich willkommen.

Torin Zander
Hallo, vielen Dank für die Einladung.

Katrin Degenhardt
Herr Zander, sagen Sie uns nochmal, was versteht man unter Cybersicherheit?

Torin Zander
Im Prinzip versteht man darunter alles, was die Sicherheit von IT-Systemen und von sogenannten OT-Systemen betrifft, also auch von heutzutage vernetzten Geräten in der

Arbeitswelt. Da geht es vor allen Dingen darum, den Systemschutz zu gewährleisten, dass keiner auf die Systeme zugreifen kann und vor allen Dingen auch keiner auf Daten zugreifen kann, wenn diese sensibel sind und schützenswert.

Katrin Degenhardt
Welchen konkreten Bedrohungen sind denn Unternehmen ausgesetzt?

Torin Zander
Das ist vielsichtig. Also zum einen natürlich auf dem digitalen Wege, das bekommt glaube ich jeder auch privat mit, dass über E-Mails versucht wird, an Daten zu gelangen, an Zugangsdaten. Ganz häufig ist natürlich auch so was wie ein Bankzugang gefährdet. Ich glaube, das hat jeder schon mal, der ein E-Mail-Postfach hat, mitbekommen, dass man aufgefordert wird, ganz dringend seine Bankzugangsdaten irgendwo einzugeben, weil irgendwas Schlimmes angeblich passiert ist und man da was tun muss.
Das sind meistens Phishing Mails, so nennt man es, die dann darauf aus sind, dass jemand Zugangsdaten erhält. Das heißt, man wird dann auf eine Webseite umgeleitet von den Angreifern, die dann vorgibt, die Banking-Webseite zu sein. Dort gibt man seine Zugangsdaten dann im schlimmsten Fall ein und der Angreifer erhält die dann und kann sich dann an der richtigen Webseite damit anmelden und gegebenenfalls zum Beispiel Zahlungen anweisen.

Katrin Degenhardt
Und die werden auch immer perfider, diese Mails.

Torin Zander
Genau, also meistens mit ganz viel Druck, der aufgebaut wird, von wegen, „Sie müssen sofort handeln und es ist ganz dringend, dass Sie das jetzt sofort machen, weil sonst Ihr Konto gesperrt wird“, zum Beispiel, das ist so eine ganz übliche Masche.

Katrin Degenhardt
Wie hängen denn digitale Sicherheit und physischer oder auch psychischer Arbeitsschutz zusammen?

Torin Zander
Man bekommt sehr viele E-Mails heutzutage. Als Beispiel, wenn man 100 E-Mails im Postfach hat, die alle ungelesen sind, der Arbeitstag ist acht Stunden lang im Normalfall, dann möchte man die alle abarbeiten, im besten Fall. Und dann entstehen vielleicht Flüchtigkeitsfehler oder man fühlt sich dann halt dadurch gestresst, dass man nicht alles abarbeiten kann, was man beantworten muss und wenn dann vielleicht Flüchtigkeitsfehlern dazu kommen, dass das einfach durchrutscht, dass irgendeine E-Mail beantwortet wird, die eigentlich gar nicht hätte beantwortet werden sollen, weil sie halt keine echte, sondern eine Phishing-Mail ist.

Katrin Degenhardt
Genau, und davor hat man natürlich Angst und das baut natürlich dann einen psychischen Druck auf. Und physischer Arbeitsschutz, also ich denke jetzt zum Beispiel an Maschinen, dass die vielleicht durch Cyberangriffe in irgendeiner Form manipuliert werden könnten.

Torin Zander

Genau, also da gab es vor ein paar Wochen in Norwegen einen Vorfall. Ich weiß nicht, ob Sie das mitbekommen haben. Da ist eine Talsperre angegriffen worden, erfolgreich gehackt worden. Da ist ein Passwort geleakt worden, sehr wahrscheinlich, ist noch nicht ganz klar, woran es lag. Und dort wurden dann aus der Ferne alle Ventile geöffnet, sodass die Talsperre auslief, mehr oder minder. Das ist dann auch aufgefallen nach ein paar Stunden und abgestellt worden. Aber das wäre so ein klassischer Fall, wo von außen durch ein IT-Leck eine OT angegriffen wurde.

Katrin Degenhardt
Und da können ja dann auch Beschäftigte betroffen sein zum Beispiel.

Torin Zander
Jetzt war es „nur“ Wasser, in Anführungsstrichen, was den Bach runtergelaufen ist irgendwo, was nicht gefährlich war, aber es kann natürlich alles andere sein. Es können irgendwelche Rolltore sein, die man aus der Ferne steuern kann auf einmal. Überhaupt Sicherheitsmerkmale, Kameras, die gesteuert werden. Da kann man auf einmal etwas sehen, was man eigentlich nicht sehen sollte innerhalb eines Betriebs oder vielleicht sogar in vertraulichen, geheimen Räumen. Oder Türen oder Tore sind natürlich immer sehr beliebt, kennt man auch aus Filmen, dass die oftmals gerne gehackt werden und geöffnet werden können und das ist gar nicht so weit weg. Also, wenn man Technik kauft, egal welcher Art und die kann irgendwie mit dem Internet verbunden werden, dann ist die in der Regel nicht so sicher eingestellt, wie sie sein sollte. Und das kann natürlich in allen Fällen eine Gefahr sein, wenn man sich damit nicht auskennt, dann mal eben schnell das neue Rolltor gekauft hat, das neue Garagentor, das dann ins Internet gebracht hat, weil das ganz toll über die App funktioniert und aber auch alle anderen das auf einmal steuern können.

Katrin Degenhardt
Da sind wir schon bei den Schwachstellen. Ich denke da zum Beispiel auch an veraltete Systeme und natürlich auch an den Faktor Mensch. Also, welche Rolle spielen denn Beschäftigte bei der Cybersicherheit?

Torin Zander
Ja, Beschäftigte sind natürlich auch elementar wichtig, weil sie meistens vor einem Bildschirm sitzen und oftmals die auslösende Aktion sind. Wenn eine Phishing-Mail reinkommt, ist die in den allermeisten Fällen nicht gefährlich, solange nicht die Aktion, die gewünscht ist, ausgeführt wird. Ein Anhang wird runtergeladen oder irgendeine Datei geöffnet oder ein Link angeklickt. Und Beschäftigte sollten natürlich Bescheid wissen, dass das gefährlich ist und wie sie damit umzugehen haben und das nicht auslösen, sodass die Sicherheitsmaßnahme in dem Fall tatsächlich die Sensibilisierung ist, das Bewusstsein, dass solche Attacken unterwegs sind.

Katrin Degenhardt
Gibt es vielleicht so fünf Tipps, was ist auf jeden Fall zu beachten für die Beschäftigten?

Torin Zander
Wenn man einen Absender nicht kennt, sollte man immer skeptisch sein, was für eine E-Mail dort auf einen zukommt. Im Zweifel ruft man bei demjenigen an, der die E-Mail verschickt haben soll und verifiziert das. Wenn man irgendwo ein Passwort verwendet, dann sollte man

auf jeden Fall dieses Passwort nur für eine Webseite oder für irgendeinen Dienst, den man nutzt, verwenden und nicht dasselbe Passwort im Zweifel überall verwenden. Das ist ganz gefährlich, weil wenn einmal ein Passwort bekannt wird, dann können sich Kriminelle sehr schnell an verschiedenen Diensten, die da so bekannt sind, so Google, Amazon-Konto, DHL-Konto, was auch immer es ist, damit auch oftmals anmelden. Das ist auch ein großes Problem.

Katrin Degenhardt
Was ist mit mobilem Arbeiten? Das kommt ja heute jetzt auch relativ oft vor, dass die Leute im Zug arbeiten oder irgendwo im Café. Gibt es da auch Dinge, die man beachten sollte?

Torin Zander
Ja, also natürlich ist es sehr wichtig, man, wenn man unterwegs arbeitet, man sich bewusst ist, dass man nicht alleine unterwegs ist, in den meisten Fällen. Ich denke jetzt so an den Zug, wo man vielleicht auch auf dem Tisch den Laptop aufgeklappt hat und dann dort arbeitet. Die Leute um einen herum können oftmals mit auf den Bildschirm schauen, wenn man sich da nicht gegen geschützt hat. Da gibt es natürlich Bildschirmschutzfolien, damit man nur selber auf den Bildschirm gucken kann. Aber auch, wenn man zum Beispiel telefoniert, kann jemand mithören, was man telefoniert, auch wenn man nur seine eigene Stimme laut hat, können auch da schon sensible Informationen preisgegeben werden, was man nicht möchte. Was aber für den Gegenüber vielleicht schon viel mehr Info ist, als man vielleicht denkt.

Katrin Degenhardt
Jetzt bitten wir ja unsere Gäste immer einen Gegenstand mitzubringen, der mit unserer Thematik zu tun hat. In dem Fall jetzt Cybersicherheit und Sie haben wirklich was ganz Kleines mitgebracht, was jetzt hier vor uns auf dem Tisch liegt. Vielleicht heb ich das mal hoch so. Also, es sieht ein bisschen aus wie so ein USB-Stick, ein kleiner USB-Stick. Was ist das?

Torin Zander
Das ist ein FIDO Key.

Katrin Degenhardt
Ein FIDO Key?

Torin Zander
Genau, gibt es schon seit über zehn Jahren tatsächlich. Eine Alternative zur Passwort-Anmeldung an Diensten. Das ist ein offener Standard, der wie gesagt, vor über zehn Jahren veröffentlicht wurde. Und das ist ein zertifikatsbasiertes Anmeldesystem. Das heißt, man kann diesen Schlüssel, den kann man tatsächlich als Schlüssel bezeichnen, zum Beispiel in seinen PC einstecken und wenn man sich dann bei einem Dienst anmelden möchte, zum Beispiel Google oder beim Apple-Konto, dann kann man diesen Schlüssel statt des Passworts verwenden. Und den muss man einmalig einrichten und dann kann man den für alle Dienste, die diesen Dienst nutzen, also diese FIDO-Standard unterstützen, verwenden und braucht dafür kein Passwort mehr.

Katrin Degenhardt

Man braucht kein Passwort mehr, man muss sich auch keine mehr merken in dem Sinne. Das ist ja sehr praktisch.

Torin Zander
Genau, man muss diesen FIDO Key natürlich dabeihaben. Man kann normalerweise auch mehrere Keys einrichten, weil so ein Key kann natürlich auch mal kaputt gehen und man sollte auch mehr als einen haben im besten Falle, wenn man da wirklich seine Systeme mit schützt. Ja, aber man kann ihn dann halt allein nicht dazu einsetzen. Es gibt auch welche, das ist jetzt ein einfaches Modell, die nochmal biometrisch gesichert sind. Das heißt, ich kann ihn nicht nur in den PC einstecken und er wird dann als Passwortalternative verwendet, sondern er braucht zuvor noch eine Freischaltung von mir in Form von einem Fingerabdruck zum Beispiel.

Katrin Degenhardt
Das klingt irgendwie ziemlich sicher. Sie haben das im Vorgespräch mal Identifizierungsdongel genannt. Das ist so der umgangssprachliche Begriff dafür.
Was sollte man mit Passwörtern nie machen?

Torin Zander
Also Passwörter sollte man im besten Falle nicht aufschreiben. Man sollte sie in einem Passwortmanager verwalten. Und die klassischen Fälle, die man vielleicht so kennt, dass das Passwort am Bildschirm klebt oder unter der Tastatur steht, sind schon, ich denke, offensichtlich nicht gut. Aber auch, dass man ein Passwort oder mehrere Passwörter, wenn man sie sich aufschreiben möchte, dass sie in einem Notizbuch zum Beispiel stehen und dieses Notizbuch dann irgendwie neben der Tastatur liegt oder in der Schublade direkt neben dem Schreibtisch. Das kann quasi jeder mitnehmen und dann hat er die Passwörter auch. Dann muss er sie halt einmal abtippen.

Katrin Degenhardt
Also, Passwörter nie, vor allen Dingen nicht in Computernähe, irgendwo aufschreiben und hinkleben, das auf keinen Fall.

Jetzt wollen wir noch mal ein bisschen auf die Unternehmen zu sprechen kommen. Wie gut sind denn deutsche Unternehmen ihre Einschätzung nach aufgestellt, wenn es IT-Sicherheit am Arbeitsplatz geht?

Torin Zander
Das kann man jetzt so ganz genau gar nicht beantworten, weil man natürlich auch gar nicht weiß, wie viele Vorfälle es jeden Tag wirklich gibt. Es gibt natürlich Statistiken, in denen Angriffe ausgewertet werden anhand von Antivirenherstellern und verschiedenen anderen Instituten, die das so mitbekommen, was so unterwegs ist. Auch die Netzwerkanbieter, die die großen Knotenpunkte, die ja in Frankfurt zum Beispiel sind, auswerten können ja anhand des Datenverkehrs und der Menge des Datenverkehrs ausmessen, wie viel gerade los ist und was ungewöhnlich ist.
Ein Fakt ist, dass quasi alle Unternehmen permanent angerufen werden, muss man sagen. Sei es durch E-Mails, sei es durch wirkliche Versuche, Schwachstellen zu finden, sei es aber auch durch physische Versuche, in ein Unternehmen einzudringen, um dort Netze zu kompromittieren. Auch das passiert.

Katrin Degenhardt
Ist das denn für Unternehmen jeder Größenordnung auch relevant? Also kommt das bei Unternehmen jeder Größenordnung auch vor?

Torin Zander
Ja, würde ich schon sagen. wenn jemand wirklich irgendwo rein möchte, kommt er dann über Umwege oftmals dann da rein. Und wenn jetzt ein Zulieferbetrieb, zum Beispiel Deutschland ist ja so ein Autoland, wenn jetzt da in der Automobilbranche zum Beispiel ein kleiner Zuliefererbetrieb, nenne ich jetzt mal klein, wenn er irgendwie unter 100 Mitarbeiter hat, irgendwas herstellt, was aber in den großen Konzernen verbaut wird, dann ist natürlich das im schlimmsten Fall die beste zu findende Schwachstelle für einen Angreifer, weil da vielleicht das Thema Cybersicherheit aufgrund der Größe nicht ganz so hoch aufgehängt wird wie in einem großen Unternehmen, und dann kann man versuchen über dieses kleine Unternehmen in ein großes Unternehmen einzudringen. Auch das hat es schon mehrfach gegeben. Also es gibt regelmäßig auch in der Automobilbranche Vorfälle, die allerdings aufgrund der hohen Cybersicherheit, die dort vorherrscht, meistens relativ früh erkannt und unterbunden werden, sodass es da nicht zu Vorfällen kommt, die wirklich kritisch sind.

Katrin Degenhardt
Und welche konkreten Maßnahmen würden Sie jetzt diesen Unternehmen empfehlen? Vielleicht allgemein erstmal? Ganz

Torin Zander
Ganz wichtig ist, wie eben schon erwähnt, das Thema Passwörter, dass ein Passwort wirklich ein personenbezogenes Passwort sein soll. Niemand sollte außer mir selbst wissen, welche Zugangsdaten ich für irgendeinen bestimmten Dienst habe. Ich sollte ihn möglichst individuell vergeben und der Einsatz eines Passwort-Safes wäre ratsam. Damit, wenn man jetzt keinen FIDO Key verwenden kann oder möchte, dass man zumindest die Passwörter sicher in einem Passwort-Safe gespeichert hat, also einer Software, die die Passwörter verwaltet. Wenn ich ein Passwort selber nicht kenne, dann ist das meistens sicherer, als wenn ich es im Kopf habe und es gegebenenfalls irgendwo falsch eingebe.

Katrin Degenhardt
Wie können denn speziell kleine und mittelständische Unternehmen mit einem begrenzten Budget effektiven digitalen Arbeitsschutz umsetzen? Was braucht man? Was braucht man vielleicht eher nicht? Haben Sie da auch konkrete Tipps?

Torin Zander
Also, was braucht man eher nicht ist immer schwierig in diesem Kontext. Da muss man Prioritäten setzen. Ja, es kommt natürlich auch darauf an, was die Unternehmen für eine Struktur haben. Ob sie zum Beispiel hauptsächlich per E-Mail kommunizieren oder ob sie eher telefonisch erreichbar sind. Auch beim Telefonieren kann natürlich einer anrufen, der nicht derjenige ist, für den er sich ausgibt. Da muss man eigentlich immer auf der Hut sein, einfach und immer erstmal kritisch hinterfragen, ob das, was da gerade reinkommt, auch wirklich von demjenigen ist, von dem es zu sein scheint. Das würde ich sagen, ist das Allerwichtigste, dass die Menschen, die da arbeiten, das Bewusstsein haben, dass das nicht immer alles gutgläubig verarbeitet werden sollte.

Katrin Degenhardt
Wenn es jetzt ein Unternehmen doch erwischt hat - wie merkt man das denn überhaupt und was ist dann zu tun, wer ist zu informieren, wie reagiert man darauf?

Torin Zander
Das ist auch sehr interessant, die meisten Angriffe werden nicht direkt bemerkt. Das ist tatsächlich ein großes Problem, weil Angreifer heutzutage versuchen, sich in Systeme einzunisten und so lange unentdeckt zu bleiben, wie es nur geht, um möglichst viel an Informationen zu sammeln, bevor der tatsächliche Angriff stattfindet. Manche Angriffe sollen sogar gar nicht erkannt werden, wenn man zum Beispiel Daten abgreifen möchte, wie zum Beispiel E-Mail-Adresse und Passwortkombinationen, wenn die irgendwo gespeichert sind. Wenn sowas erkannt wird, sollte man natürlich sofort die betroffenen Systeme identifizieren und diese vom Internet trennen und analysieren, ob noch weitere Systeme betroffen sind. Das machen auch viele Firmen professionell, weil das kann normalerweise ein normales Unternehmen so, ohne jetzt Cybersicherheitsexperte zu sein, nicht. Aber da gibt es dann tatsächlich Maßnahmen, die dann von außen auch ergriffen werden können.
Es gibt auch Meldepflichten für Sicherheitsvorfälle seitens des BSI. Jetzt ganz aktuell ist ja das Gesetz zur Cybersicherheit und Cyberresilienz in Deutschland in Arbeit. Da warten wir alle auf die Veröffentlichung. Und je nachdem, was da jetzt genau drinsteht, sind auch viele Unternehmen dann verpflichtet, Sicherheitsvorfälle an das Bundesamt zu melden, also an das BSI.

Katrin Degenhardt
Zum Abschluss nochmal die Frage, wir haben ja auch gesagt, wie wichtig die Beschäftigten sind und dass sie sensibilisiert sind, dass sie aufmerksam sind, aber wie können Unternehmen ihre Beschäftigten sensibilisieren? Vielleicht einfach mal als Beispiel, wie macht das die BG ETEM?

Torin Zander
Ja, also die BG ETEM hat eine Kampagne gestartet, um die Mitarbeiterinnen und Mitarbeiter zu sensibilisieren. Wir haben dafür auch einen Dienstleister beauftragt, der mit Schulungsvideos vor allen Dingen in verschiedenen Bereichen der Angriffe Videomaterial anbietet, interaktives Lernmaterial, das heißt, das sind Videos, da wird kurz die Bedrohungslage gezeigt, zum Beispiel bei den Phishing Mails, dass eine Phishing Mail reinkommt, wie sie aufgebaut ist. Und dann wird darauf hingewiesen, wie man damit umgehen soll, dass man die, wenn man sie geöffnet hat, prüfen soll, von wem sie ist, wie man das prüfen kann.
Ja, und zum Zweiten, das ist dann die Bewusstseinsschärfung im Sinne von Schulung, klassisch lernen, wie in der Schule so ungefähr. Dann gibt es aber auch die Beispiele, dass wir aktiv hingehen und Fake-Phishing-Mails an die Mitarbeiterinnen und Mitarbeiter verschicken, die dann halt, wenn man sie dann anklickt, die Links, die dann auf einer Plattform, die natürlich nicht gefährlich ist, landet, die dann das Bewusstsein schärfen soll, also die dann quasi die Schulung nochmal verdeutlicht, dass die Inhalte vermittelt werden, warum man diese E-Mail jetzt hätte nicht anklicken sollen, warum die gefährlich ist.

Katrin Degenhardt

Das ist ja eine sehr nachahmenswerte Methode, weil ich glaube, da lernt man sehr viel dabei.

Torin Zander
Ja, definitiv. Also es gibt auch immer mehr Leute, auf diese gut gemachten Phishing-Mails reinfallen. Ich selber muss auch ab und zu mal gucken, weil ich natürlich auch nicht immer weiß, was für Mails durch das Unternehmen da verschickt werden. Und ja, die Trefferquote wird tatsächlich mit den immer besser werdenden Phishing-Mails auch bei diesen Fake-Mails relativ hoch. Wir sind dabei teilweise 20 Prozent der Belegschaft, die diese E-Mails doch noch anklicken.

Katrin Degenhardt
Und jetzt haben wir ja auch noch, jetzt kommt ja noch KI hinzu. Da kommt ja jetzt zum Beispiel auch bei Anrufen dieses sogenannte Voice-Cloning. Wie kann man denn darauf reagieren, beziehungsweise wie kann man das denn erkennen, wenn es so Phishing-Anrufe gibt mit geklonten Stimmen?

Torin Zander
Ja, das ist tatsächlich ein Problem, das sehr aktuell ist. Dafür benötigt man, wenn man so etwas machen möchte, wenn es ein Live-Anruf ist, sag ich jetzt mal, und kein aufgezeichnetes Band abgespielt wird, dann könnte man es vielleicht daran hören, dass mal irgendwo was kracht im Hintergrund oder dass die Stimme mal nicht 100%, ich nenne es mal übersetzt wird, weil es wird ja von jemand anderem normalerweise gesprochen und ein System versucht, das live zu transkribieren.

Da könnte man, wenn man ganz genau hinhört, heraushören, aber ich glaube tatsächlich, dass das sehr schwierig ist. Weil in den meisten Fällen bei so einem Voice-Anruf dann Druck aufgebaut wird in Form von, „hallo, wir müssen sofort handeln“. Man kennt das vielleicht vom Enkeltrick. Wenn der Opa angerufen wird, dann heißt es immer, ist zum Beispiel ein Unfall passiert und da muss jetzt sofort jemand 10.000 Euro von der Bank abheben, weil wir müssen da sofort irgendwas bezahlen.

Katrin Degenhardt
Also, das heißt, da muss auch die Cybersecurity sich weiterentwickeln und muss Methoden finden, wie man sich auch davor schützen kann. Sie haben auch noch den QR-Code angesprochen. Auch da besteht ja Gefahr. Gibt es denn überhaupt eine Möglichkeit zu erkennen, ob ein QR-Code jetzt sicher ist oder nicht?

Torin Zander
Wenn ich einen QR-Code jetzt zum Beispiel am Laternenpfahl sehe, dann sollte man darauf achten, dass der nicht einfach nur alleine da hängt und man ihn abfotografiert, sondern dass zumindest die Domain, also die URL, die da aufgerufen wird, einmal unten drunter abgedruckt ist. Und wenn man das mit dem QR-Code-Scanner abfotografiert, dann wird das in den meisten Fällen als Vorschau, bevor man den tatsächlich abruft, angezeigt. Und da kann man dann schon gucken, ob das übereinstimmt. Und wenn das nicht übereinstimmt, dann ist es in den meisten Fällen wahrscheinlich kein valider QR-Code.
Wenn man jetzt beim Online-Banking speziell schaut, das ist eine sehr häufige Masche im Moment, die rumgeht, dass Rechnungen herumgeschickt werden, wo dann ganz unten

rechts der QR-Code zum „Hier können Sie schnell Online-Banking überweisen, die Vorlage einfach nur abfotografieren und überweisen drücken“, nutzen, da sollte man dann tatsächlich die Werte, die das System dann vorausfüllt, mit denen, die auf dem Brief hoffentlich auch noch draufstehen, mit IBAN und Rechnungsbetrag und Empfänger abgleichen, da ganz sicher zu gehen, dass das nicht an das falsche Postfach oder das falsche Konto geht.

Katrin Degenhardt
Ja, also ich glaube, da haben wir jetzt sehr viel erfahren und ich glaube auch vieles ist sowohl für Unternehmen und für Privatpersonen gleichgültig, kann man so sagen, was Cyberkriminalität angeht. Dann bedanke ich mich ganz herzlich bei Ihnen, Herr Zander, danke, dass Sie bei uns zu Gast waren.

Torin Zander
Sehr gerne, danke für die Einladung noch mal.

Katrin Degenhardt
Und hier noch drei Takeaways für Ihre Sicherheit.

- Erstens, immer unterschiedliche Passwörter benutzen und diese im Passwort-Safe sichern. Eine gute Alternative wäre auch ein FIDO Key.

- Zweitens, grundsätzlich sollte man misstrauisch gegenüber E-Mails mit drängenden Aufforderungen sein und bei Unsicherheiten lieber einmal zu viel bei der IT-Abteilung nachfragen.

- Und drittens, beim Arbeiten unterwegs daran denken, dass man nicht alleine ist.

Und wir freuen uns natürlich, liebe Zuhörerinnen und Zuhörer, wenn Sie uns auf dem Podcast-Kanal Ihrer Wahl abonnieren und uns eine Bewertung oder einen Kommentar und gerne auch Fragen dalassen. Weiterführende Informationen finden Sie auch in den Shownotes und unter etem.bgetem.de

Festzuhalten bleibt, digitale Sicherheit erhöht auch die allgemeine Sicherheit in Unternehmen und kommt allen Beschäftigten zugute.

Investitionen in passende Schutzmaßnahmen und die Sensibilisierung für Cybergefahren zahlen sich aus. Ganz sicher.

Outro
Ganz sicher. Der Podcast für Menschen mit Verantwortung.