10/20/2025

Science Talk > Phishing, Deep Fakes, Internetbetrug: Cybersicherheit geht uns alle an. Was sagt die Wissenschaft, was tun die Hochschulen?

00:00:01 **Speaker 0**

So, schönen guten Abend. Hier ein vorletztes Mal im Jesuitensaal der Aula der Wissenschaften, zumindest was unseren Science Talk anbelangt, den Science Talk des Bundesministeriums für Frauen, Wissenschaft und Forschung. Äh, wir sind ab 2026 nämlich, äh, gezwungen, in die TU zu übersiedeln, hoffentlich gemeinsam mit Ihnen. Dort werden wir dann ein Jahr lang unsere Science Talks monatlich abhalten. Ich fange jetzt schon an, das rechtzeitig zu sagen, damit dann nicht 2026 irrtümlich uns jemand hier sucht. Also ich hoffe, Sie bleiben uns treu. Das ist einmal die für mich, äh, fast wichtigste Nachricht, sozusagen, dass Sie alle gemeinsam mitzunehmen, äh, wenn hier dann das Austrian Centre of Science Communication entsteht. Vielleicht kommen wir ja 2027 dann hierher wieder zurück. Heute widmen, äh, wir uns einem komplexen Thema. Das ist eh fast jedes, das sagt sich so leicht dahin, äh, aber einem Thema, das lange Zeit jetzt schon in aller Munde ist. Wir selber als Bundesministerium haben eine

00:01:18 **Speaker 0**

kleine Kampagne gemacht zu Cyber Security und vor allem die Universitäten und die Uniko, also die Universitätskonferenz, haben sich gemeinsam zu einem Resilience Plan und Act, äh, verabschiedet, zusammengetan, zusammengeschlossen, äh, der sehr vieles von dem sicherstellen soll, wo es in der Cyberkriminalität manchmal vielleicht noch Lücken gibt. Die heutige Diskussion leitet Astrid Kuffner. Ich darf sie kurz vorstellen. Sie ist Wissenschaftsjournalistin, unter anderem auch bei APA Science tätig. Und ich würde Sie gerne auf eins aufmerksam machen, nämlich einen Podcast, den ich selber jetzt ein paar Mal gehört habe. Nie ganz fertig, aber er war jedes Mal so dass ich mir gedacht habe, ich muss das Ende doch noch hören. Und der heißt „Nerds mit Auftrag". Stimmt das, Frau Kuffner? Ja, gut. Okay. Und von den Nerds abgeleitet komme ich eigentlich, äh, zu dem Faktor, der in dieser ganzen Cyber-Security-Geschichte vielleicht der Faktor ist, den wir nicht immer bedenken. Äh, das Einfallstor, glauben

00:02:38 **Speaker 0**

wir immer, ist nur eine Frage der IT-Sicherheit. Vielleicht ist es aber auch eine Frage des menschlichen Faktors, nämlich der-- das Vertrauen, das wir haben, oder auch das Misstrauen, ähm,

das wir dem entgegenbringen sollen. Also vielleicht wird das heute ein soziologischer Prozess gemischt mit viel IT. Ich wünsche Ihnen einen schönen Abend.

00:03:09 **Speaker 2**

Danke, Martha Brinek, für die freundliche Vorstellung und die Eröffnung des Science Talks namens unseres Gastgebers, des Bundesministeriums für Frauen, Wissenschaft und Forschung. Ich wünsche uns allen einen schönen Abend. Herzlich willkommen auch von mir. Unser Thema heute in der Aula der Wissenschaften und auch im Livestream: Phishing, Deepfakes, Internetbetrug, Cybersicherheit geht uns alle an. Was sagt die Wissenschaft? Was tun die Hochschulen? Kein kleines Thema, das wir uns da heute vorgenommen haben. Eigentlich sehr viele auf einmal. Wie das alles zusammenhängt und warum Universitäten, Hochschulen, äh, ein guter Ort sind, um dieses Thema zu verhandeln, weil sie auf der einen Seite sehr offen sein müssen, um ihre Aufgaben zu erfüllen, auf der anderen Seite selber Angriffsziel sein können für Cyberkriminelle, weil sie einfach sehr reiche und attraktive Datenquellen sind, aber auch Teil der Lösung, weil sie Sicherheitsfachkräfte ausbilden und technische Lösungen weiterentwickeln. Das

00:04:08 **Speaker 2**

möchte ich heute mit einer hochkarätigen Runde besprechen, die ich Ihnen kurz vorstellen darf. Ich beginne ganz außen, flankierend zu mir, Anna Wimmerzahl. Sie ist seit 2007 Assistenzprofessorin für Kryptografie, SmartCard-Systeme und digitale Ide-Identitäten an der FH Hagenberg. Sie bildet also den Nachwuchs an IT-Security-Fachkräften aus. Ganz aktuell hat sie mit ihrem Kollegen ein Lehrbuch zu Kryptografie veröffentlicht und sie ist Teil des Quantum und Postquantum Labs. Sie hat selbst an der FH Hagenberg studiert, und zwar sichere Informationssysteme. Dann in der Mitte, sozusagen von den Gästen, Gerald Steiner. Er ist Chief Information Officer der Universität Salzburg und hat, äh, mein volles Mitleid. Das ist bestimmt kein leichter Job. Im Rahmen des eben verands-- äh, verabschiedeten Cyber Resilience Plans für die öffentlichen Universitäten in Österreich ist die Uni Salzburg auch einer der Projektpartner, die im Bereich Awareness und Training tätig werden sollen. Er ist Vorsitzender

00:05:11 **Speaker 2**

der ARG CIT. Das ist die Vereinigung aller CIOs, aller zweiundzwanzig öffentlichen Universitäten und er hat selbst technische Informatik an der Hochschule Mittweida und den MBA im Bereich Innovation und Entrepreneurship an der WU Wien absolviert. Und gleich hier an meiner Seite ist Helmut Leopold. Er leitet seit 2009 das Center for Digital Safety and Security am Austrian Institute of Technology AIT, das er zu einem international anerkannten Cyber-Security-Forschungszentrum

aufgebaut hat. Er bringt mehr als drei Jahrzehnte Managementerfahrung mit im Bereich IT, Telekommunikation und Digitalisierung und er hat an der TU Wien Informatik studiert und promoviert in Computer Science an der Universität Lancaster in England. Ich sage jetzt noch drei Worte zum Ablauf. Wir bemühen uns, dieses, äh...Das massive Thema hier ein bisschen in den Überblick zu kriegen, in den Griff zu kriegen, wollen aber dann gerne sozusagen die Runde öffnen für Ihre Fragen. Wir haben Saalmikros, das heißt, äh, wenn wir

00:06:14 **Speaker 2**

ins Publikum gehen mit den Fragen, warten Sie bitte, wie das Mikro bei Ihnen ist, damit wir Sie gut hören können. Und wir haben vorab auch schon eine Frage aus dem Livestream bekommen, die ich dann auch gerne stellvertretend stelle. So, jetzt aber es geht los. Vor vierzig Jahren wurden die ersten E-Mails verschickt an der Universität Wien über sündteure Großrechner. In der Zwischenzeit ist viel passiert, das muss ich jeder nicht sagen. Die fiebernden Modems sind schon ausgestorben. Mails gibt es immer noch, Browser, es hat sich alles ausgewachsen zu einer umfassenden Digitalisierung der Gesellschaft mit Smartphone in der Hosentasche und Glasfaser bis ins letzte Tal. Ähm, das sind durchaus Segnungen, die wir da erfahren haben, aber ich möchte trotzdem mit dem Problemaufriss beginnen, und zwar mit Ihnen, Herr Steiner, CIO der Universität Salzburg. Vierzig Jahre nach den ersten Mails, äh, worin bestehen denn Ihres Erachtens die größten Herausforderungen, mal ganz grob gesprochen, in der IT-Sicherheit?

00:07:14 **Speaker 2**

Zeigen sich vielleicht gerade an den Hochschulen auch Probleme, die Unternehmen haben, die auch Privatpersonen haben, vielleicht sogar wie unter einem Brennglas?

00:07:22 **Speaker 3**

Ja, danke. Einen schönen guten Abend wünsche ich alle. Ähm, die Problematik, die an Universitäten ist, kann man nicht zu hundert Prozent mit, mit einem klassischen Unternehmen auch vergleichen. Ah, Universitäten haben mehrere Divisions, die, die in der Organisationseinheit abgebildet sind. Wir haben klar vier Aufgaben. Das ist sozusagen Lehre, Forschung, Verwaltung und sozusagen die third mission zu adressieren als Universitäten. Und überall sozusagen haben wir, ah, Themen, die uns sozusagen von außen auf, auf die Sicherheitsebene betreffen. Ähm, für Universitäten aber ein sehr wichtiger Punkt ist sozusagen, die Kernprozesse der Universität, äh, aufrechtzuerhalten und diese auch sozusagen zu, zu schützen, damit dass Lehre, Forschung und Verwaltung gut miteinander arbeiten können und auch, äh, interdisziplinär untereinander arbeiten können. Die

Herausforderungen sind auf, auf allen Ebenen unterschiedlich. Es gibt sozusagen auch einerseits die technischen Herausforderungen, die wir adressieren

00:08:31 **Speaker 3**

müssen, die natürlich sozusagen, äh, sehr, äh, mannigfaltig sind und wo ich aber sage, die können wir am einfachsten lösen. Dann haben wir natürlich die organisatorischen Herausforderungen. Äh, Universitäten sind ja in sich per se Ökosysteme, äh, und diese Ökosysteme, äh, müssen auch sozusagen funktionieren und dazu braucht's Prozesse, Abläufe, äh, Kooperationen, zweiundzwanzig Universitäten, die sozusagen auch, äh, zusammenarbeiten. Wenn man jetzt noch ein bissl weiter denkt auf europäischer Ebene, äh, wollen wir sozusagen ja auch, äh, internationale Studierende bei uns attraktiveren. Und alle diese Themen haben natürlich ein, eine rießen Facette an Angriffsmöglichkeiten und, äh, Security-Themen. Es geht von Data Privacy on bis zu hin zu klassischen, äh, Sicherheitslücken. Die Software, die wir einsetzen an Universitäten, auch da schon eine Riesenmannigfaltigkeit an, an, an Software, die wir, die wir bedienen müssen. Und diese gilt es heut am, ah, zu lösen und zu beschreiben. Und die

00:09:49 **Speaker 3**

Lösung führt über Kooperation. Das heißt, wir werden die Thematik nicht alleine lösen als Universität Salzburg, äh, wir werden sie sozusagen in Kooperation mit allen zweiundzwanzig Universitäten adressieren und dadurch sozusagen auch die Möglichkeit, ah, zu schaffen, sozusagen Ressourcen zu nutzen, Synergien zu heben und dergleichen. Und alle diese Themen müssen wir sozusagen technisch, organisatorisch und prozessual begleiten. Und dann glaube ich, können wir das sozusagen auf, auf guter Basis lösen.

00:10:25 **Speaker 2**

Technische Herausforderungen sind am einfachsten zu lösen. Ich habe mir das aufgeschrieben. Mhm Ich komme da noch darauf zurück. Herr Leopold, Sie waren, bevor sie am AIT tätig war- tätig, äh, geworden sind, auch Technologiechef der Telekom Austria unter anderem verantwortlich für die Einführung des Breitbandinternets in Österreich. Danke dafür. Welche Schattenseiten dieser Internetdurchdringung beobachten Sie denn mal so als aus der Vogelperspektive, ohne schon ganz in der letzten Verwinkelung zu landen?

00:10:56 **Speaker 4**

Wir haben ausgemacht, dass wir nur ganz kurze Antworten geben sollen. Die Frage ist unfair, weil da kann man eine lange Antwort sein. Nein, ähm, zusammenfassend ist die Frage jetzt und bringt auf

den Punkt und auch nachgehen, was du gesagt hast, äh, Gerald. Wir haben damals das Internet, also ich gehe zurück, Jahre neunundachtzig hat es begonnen, achtundneunzig dann Breitband, äh, wo wir heute sind. Und das war eigentlich immer nur eine positive Botschaft. Alles wird besser, weil wir endlich, was auch passiert ist und wir erreicht haben, eine unheimlich coole Informationsverteilmaschine gebaut haben. Davor war es vor fünfhundert Jahren durften nur, wir konnten nur wenige lesen und Bücher von Hand schreiben. Dann kam Buchdruck und dann kam das Thema, dass nur wenige die Macht hatten, Zeitungen, Medien. Und da war diese Demokratisierung, jeder wird zum Produzenten und zum Konsumenten. Das ist das Wort des Prosumers. Das haben wir erreicht. Jeder kann heute jedem alles sagen. Das ist das Internet.

00:11:57 **Speaker 4**

Also diese gute Botschaft haben wir gebaut. Was ich selbstkritisch auch mit sagen muss, die gesamte Community weltweit hat übersehen, dass damit auch ähm-Eine Verantwortung kommt und ein möglicher Missbrauch. Und den erleben wir halt, wenn wir das Thema Desinformation arbeiten. Also ich glaube, wir haben heute mit dem Internet die größte Desinformationsmaschine, die die Menschheit je hatte, was uns vor riesigen gesellschaftlichen Herausforderungen noch bringen wird, weil wir nichts mehr glauben können, was da draußen auf uns zukommt und wir leider alle Opfer Mögliche sind, weil wir uns zu eng in unserer Filterblase informieren, Informationen schicken lassen, sind wir auf dieser Informationsmanagement-Ebene. Das ist der eine Problembereich. Der zweite ist, wenn wir auf das Thema Sicherheit retour gehen, soll ich das vielleicht noch mal kurz am Punkt bringen? Aus meiner Sicht, warum haben wir heute ein Problem? Wir haben eben dieses Internet gebaut mit einem sehr gutgläubigen Ansatz, alle

00:12:54 **Speaker 4**

global auf der Welt. Das ist das Gleiche gewesen. Das wird nur für das Positive verwendet. Wenn wir heute, wenn Sie einen PC zu Hause oder ein Smartphone einschalten, dann ist da draußen mittlerweile ein enormer Aufwand entstanden von der negativen Seite der Welt. Das sind auch keine Menschen mehr, sondern eine groß angelegte Industrie, die nichts anders tut, die versucht, auf unsere Geräte zu kommen. Punkt. Ob das jetzt kriminelle Motivation ist, kann man sich Innenministerium fragen, wie die Crime-Zahlen hinaufgehen im Vergleich zum Physischen, ob das terroristische Aktivitäten sind, ob das einfach jemand will, ihm einen Schaden zufügen, bis hin jetzt globale Weltsituation. Also das ist eine unheimliche Macht draußen, die nichts anders tut, Werkzeuge, die gebaut wurden, die nichts anders tun, auf unsere Geräte zu kommen und uns zu schädigen, Daten zu stellen, unsere Geräte stillzulegen. Und da müssen wir jetzt – und das ist für mich schon eine zeitliche Änderung jetzt –, auf das müssen

00:13:51 **Speaker 4**

wir jetzt auch reagieren, wie wir die Technik bauen. Das ist mein letzter Punkt, weil da hat sich im Wesentlichen salopp sind, die letzten 40 Jahre nichts geändert. Wir bauen immer noch Technik. Ein Techniker geht her, schreibt an eine ... Ein Informatiker geht her, schreibt an Line of Code und dann bauen wir Systeme, die Millionen Lines of Code haben. Kein Mensch, kein Ingenieur, würde ich sagen, versteht heute mehr diese großen komplexen Systeme, die wir bauen. Und dadurch wird es implizit wieder ein Sicherheitsrisiko.

00:14:22 **Speaker 2**

Das klingt jetzt schon nicht mehr so einfach zu lösen. Frau Wimmerzahl, was gibt es vom Campus Hagenberg zu berichten, wo ja viel digitale Kompetenz gebündelt ist? Sind denn Ihre Studierenden wenigstens gegen Cyberattacken besser gewappnet oder ist es dann im eigenen Haus eh so wie bei allen anderen auch?

00:14:44 **Speaker 5**

Ich sage einmal: Jein. Ich denke, das ist die beste Antwort. Hallo auch schon wir an alle. Ich denke schon, dass gerade bei uns am Studiengang sicher Information System ein höheres Bewusstsein herrscht für diese Thematik, ganz klar. Ich möchte aber dazu sagen, dass niemand, gar niemand gefeit ist vor einem Cyberangriff, also auch nicht unsere Studierende, gerade wenn ich an Phishing-Angriffe denke, wenn die gut gebaut sind und man Stress hat oder gerade aufgewacht ist oder gerade schlafen geht oder gerade an etwas anderes denkt, dann kann das wirklich jedem und jeder Person passieren und da muss Man muss sich auch nicht dafür schämen, sondern mein Punkt – und da möchte ich gerne den Kollegen anschließen – ist, das müsste man anders lösen. Man müsste das viel technischer lösen und man müsste sich von diesen alten Systemen vielleicht auch trennen und sagen: „Gut, es kann mir einfach nicht jeder eine E-Mail schreiben und nicht jede, sondern nur die Leute, die in meinem Adressbuch stehen. Dann

00:15:44 **Speaker 5**

würden schon ganz, ganz viele Phishing-Mails wegfallen, aber auf das wollen wir nicht verzichten. Wir wollen ja Newsletter bekommen. Wir sind das gewohnt. Wir wollen, dass uns andere kontaktieren, neue Personen kontaktieren. Wir wollen auf Links in E-Mails klicken. Dafür war E-Mail nie gedacht. Das haben wir zu einem schönen bunten Ding ausgebaut, wo man jetzt draufklicken kann. Man sieht gar nicht mehr, was sich hinter dem Link versteckt, aber wir klicken drauf. Das stammt noch aus der Zeit, aus diesem positiven Internet. Heutzutage müsste man sagen, Links in E-

Mails gehören verboten. Also dann hätten wir kein Phishing-Problem, zumindest nicht per E-Mail, über andere Applikationen dann wieder doch. Also ich denke, man muss da die Technik auch neu denken. Man muss da neue technische Lösungen finden. Man darf nicht alles auf die Benutzer und Benutzerinnen abwälzen. Aber, und das ist leider das Große aber, zu guter Letzt bleibt trotzdem noch dieser letzte Faktor Mensch, denn wenn wir es so

00:16:39 **Speaker 5**

sicher machen, dass wir die Anwendungen nicht mehr nutzen können, so wie wir sie nutzen wollen, dann sind wir ja auch nicht zufrieden. Also dann habe ich zwar eine super sichere Applikation, aber ich werde sie nie wieder verwenden, weil die Anmeldung zu kompliziert ist, weil die Applikation nicht das macht, was ich gerne hätte. Und insofern ist das immer ein Abwägen zwischen Sicherheit und Benutzbarkeit. Und was wollen die Nutzer und Nutzerinnen? Genau.

00:17:06 **Speaker 2**

Das ist eine geheime Theorie von mir schon seit Jahren. Sicherheit und Bequemlichkeit wohnen auf verschiedenen Planeten. Gut, ich wäre jetzt, weil wir beim Problemaufriss sind, noch ein bisschen das Grauen verstärken, bevor wir uns dann auf die Ebene der Lösungen begeben. Also Zahlen bitte Cyberattacken nehmen in Österreich rapide zu. Laut Cybersicherheitsbericht 2023 wurden 65.864 Internetdelikte angezeigt. Das sind 9,4% mehr als im Jahr davor, in nur einem Jahr. Die Dunkelziffer ist sicher höher, wobei wir schon gehört haben, es gibt keinen Grund, sich zu genieren. Es kann wirklich jedem passieren. Kpmg hat eine Studie Cyber Security in Österreich aus 2024 herausgegeben und darin steht, dass jeder siebte Angriff auf ein Unternehmen erfolgreich war. Jetzt habe ich noch, damit Sie es alles einmal gehört haben und weil es auch im Titel ist, damit das nicht so mysteriös bleibt, die Top fünf Angriffsarten. Dann, verspreche ich, kommen wir zu den Lösungen. Platz eins: Phishing-Attacken.Das

00:18:15 **Speaker 2**

ist sozusagen, bekommt eine betrügerische E-Mail, eine Textnachricht, einen Telefonanruf, ein WhatsApp und Menschen werden dazu verleitet, sensible Daten wie Identität, Passwörter, Adressen oder Bankdaten weiterzugeben oder Schadsoftware herunterzuladen. Häufig werden aktuelle Themen als Aufhänger benutzt oder vorgetäuscht, dass die Bank, die Behörde oder ein Anbieter oder Willhaben oder die Post oder das Finanzamt in Wirklichkeit die Nachricht geschickt hat. Ich mache mal eine kurze Umfrage: Wer hat schon mal so ein gefaktes Postmail bekommen? Jaaa.

00:18:50 **Speaker 0**

Wer hat draufgedrückt?

00:18:52 **Speaker 2**

Nein, das fragen wir nicht. Wer hat es bekommen? Wer hat schon mal so ein gefaktes Willhaben-Mail bekommen? Ihr Paket hängt irgendwo. Sie müssen jetzt sofort Geld überweisen, damit das Paket zugestellt wird. Ja, auch bekannt. Gut. Äh, PayPal? Ihr PayPal-Konto braucht dieses und jenes. Ich bin dann immer froh, dass ich nicht PayPal habe. Dann weiß ich, das muss Mist sein. Oder die Bank. Bitte geben Sie jetzt auf der Stelle Ihre Verfügung-Nummer und Ihren was auch immer und Ihren IBAN und alles ein. Okay, die Banken scheinen doch ganz gut zu informieren. Ja, also es wird immer besser. Gut, wir waren bei den Top fünf Angriffsarten, Platz zwei Malware, also Schadsoftware oder missbräuchlich eingesetzte Tools, die Daten ausspionieren und abgreifen, den Datenverkehr manipulieren, zum Beispiel beim Online-Banking, oder Erpressungen ermöglichen, die sogenannte Ransomware. Häufig in einem Anhang oder mit einem Link versehentlich aktiviert, steht hier in meinen Unterlagen. Platz drei: Business E-Mail-Compromise

00:19:54 **Speaker 2**

beziehungsweise CEO-CFO-Fraud. Eine Betrugsmasche, bei der sozusagen unter Verwendung falscher Identitäten zur Überweisung von Geld zum Beispiel manipuliert werden soll. Der Chef ruft vermeintlich an, gerne auch mit einer KI-generierten Stimme oder schickt eine Anweisung per Mail, dass man jetzt sofort auf ein argentinisches Konto soundso viel Euronen überweisen soll, damit irgendwas, äh, passiert. Social Engineering auch dabei bringt Menschen dazu, Informationen weiterzugeben und Fehler zu begehen, die ihre Sicherheit oder die des Unternehmens gefährden, in dem Druck ausgeübt wird und die Person direkt angesprochen wird. Wer hat das WhatsApp bekommen? Äh, das Kind ist im Ausland und hatte einen Unfall? Ja, auch bekannt. Okay. Ähm, ja, der Reiche... Wir wären ja froh, wenn wir immer noch die Mails von den reichen Prinzen aus irgendwo kriegen würden, nicht die... Das wissen wir schon, dass die im Regelfall nicht gibt. Okay, und Platz fünf, äh, das Best of Böse sozusagen: Distributed Denial

00:20:57 **Speaker 2**

of Service-Attacken, DDoS-Angriffe, wo sozusagen durch wiederholte Anfragen automatisiert das Zielsystem überlastet und das eigentliche Service lahmgelegt wird. So, jetzt wissen wir es. Wird also Zeit, dass wir ganz schnell zu den Beiträgen und Lösungen kommen. Frau Wimmerzahl, ich würde gerne mit Ihnen beginnen. Sie bilden Expertinnen für Cybersicherheit aus in Hagenberg, die in Unternehmen gehen, die Produkte und Anwendungen sicher machen sollen. Wie bleiben Sie da in

der Lehre auf dem neuesten Stand? Denn es scheint ja ein permanenter Wettbewerb zu sein zwischen Gepard und Gazelle.

00:21:31 **Speaker 5**

Ja, das macht ja auch die Lehre bei uns so besonders spannend. Also, es ist nie langweilig bei uns. Ähm, und das kommt automatisch auf uns zu, auch durch die Studierenden. Also die bleiben ja auch am Ball und die konfrontieren uns damit und sagen: „Oh, da ist was passiert. Können wir uns das näher anschauen? Können wir da ein Projekt machen?" Ähm, und auch selber natürlich verfolgen wir ganz stark was, was passiert, damit wir da am Stand der Technik bleiben. Ähm, und wir freuen uns natürlich, dass viel passiert, ähm, weil so gibt's für unsere Absolventen und Absolventinnen immer viel zu tun. Äh, also das ist natürlich immer so ein, ähm, Geben und Nehmen. Also wir-- Natürlich ist es tragisch, wenn etwas passiert. Umgekehrt können wir uns dann wieder mit diesen neuen Dingen beschäftigen, wieder Lösungen für neuartige Angriffe finden, äh, und es bleibt spannend.

00:22:18 **Speaker 2**

Okay, also das eine freut das andere leid.

00:22:20 **Speaker 5**

Genau.

00:22:20 **Speaker 2**

Wenn wir jetzt über Beiträge und Lösungen, ähm, reden, was würden Sie denn sagen, was kann jetzt Technik für uns tun in diesem Bereich, in diesem Sicherheitsbereich?

00:22:30 **Speaker 5**

Ja, Technik könnte und kann sehr viel, viel tun. Also gerade im Bereich Phishing, da gäbe es schon Authentifizierungslösungen, ähm, die nicht phishbar sind. Also wenn alle Applikationen die verwenden würden, ähm, dann wäre Phishing im Web kein großes Thema mehr. Das Problem ist wieder die Benutzbarkeit dieser Dinge. Ich habe das auch selbst schon ausprobiert, diese neuen Passkeys, die es jetzt gibt. Die Idee ist eine sehr einfache. Ähm, ich brauche nur mein Handy. Die Registrierung ist ganz einfach. Ich scanne nur einen QR-Code und ab dann kann ich mich mit dem Handy Phishing-sicher anmelden. So die Theorie. In der Praxis ist es leider so: Es gibt wieder viele verschiedene Hersteller, es gibt viele verschiedene Interessenten. Ähm, ich habe auf meinem Handy jetzt die Möglichkeit, verschiedene Passkey-Provider auszuwählen. Wenn ich mich jetzt bei meinem Microsoft-Konto einen Passkey hinterlegen möchte, sagt Microsoft, ich muss dafür eine App installieren. Jetzt muss ich zuerst die App installieren,

00:23:27 **Speaker 5**

dann muss ich dort mein Microsoft-Konto hinzufügen. Dann kann ich den QR-- Nein, nein. Dann muss ich in den Einstellungen noch aktivieren, dass diese App ein Passkey-Provider ist. Dann kann ich den QR-Code scannen und dann bin ich am Ziel. Und dann bin ich maximal verwirrt, weil ich weiß auch nicht, wo werde ich zukünftig meine anderen Passkeys, die nicht mit meinem Microsoft-Konto, sondern mit einem anderen Konto verknüpft sind, wo werde ich die hin speichern? Ähm, ich sehe da ein großes Problem, dass da jetzt schon wieder so viele mitmischen in unserem heterogenen Internet, wo jeder dabei sein möchte und jeder das anbieten möchte, ähm, dass der Benutzer oder die Benutzerin wieder auf der Strecke bleibt. Also ich war verwirrt, muss ich sagen, wie ich mir das eingerichtet habe. Und dann denke ich mir: Ja gut, wie soll das jetzt, äh, meine Oma? Ja, machen. Ähm, das kann ich mir beim besten Willen nicht vorstellen. Das muss noch einfacher werden und das könnte einfacher sein, wenn es nicht

00:24:19 **Speaker 5**

so viele verschiedene Interessen gäbe.

00:24:21 **Speaker 2**

Okay, okay, das ist also meine Theorie mit der Bequemlichkeit versus Sicherheit findet hier gerade Bestätigung. Herr Leopold, Sie arbeiten mit Organisationen zusammen, wo wir alle definitiv nicht wollen, dass sich jemand ungefragt Zutritt verschafft. Internationale Atomenergiebehörde zum Beispiel, Vienna Center for Disarmament and Non Proliferation oder Büro der Vereinten Nationen für Terrorismusbekämpfung. Da, also, ich glaube, Sie stimmen mit mir überein, dass wir nicht möchten, dass da irgendjemand in den Systemen herumfuhrwerkt und etwas herausholt, was ihn nichts angeht. Hmm, ja, wenn wir mal bei der Technik bleiben, gibt es technische Lösungen, die Sie empfehlen? Sehen Sie da Möglichkeiten?

00:25:02 **Speaker 4**

Also ganz klar, ja. Und du hast es schon angesprochen: So wie wir es heute machen, unendlich kompliziert ist es wohl-- ein Gleichnis wäre, wir steigen ins Auto ein und müssen zuerst die Zündkerzen zurechtschleifen und noch drei Stunden kontrollieren... Lassen wir, drücken drauf und fahren. Das Auto ist ein gutes Beispiel, die Technik ist versteckt vor uns. Das müssen wir erreichen. Das haben wir in diesem ganzen Internetthema nicht. Es ist viel zu kompliziert, darum diskutieren wir das auch und haben wir das Problem. Das muss sich aber bessern. Vielleicht ganz kurz: Wo sind zwei große Probleme, die wir haben auf der technischen Seite? Das eine ist, wir reden jetzt hier, als

Informatiker kann ich das sagen, wir schreiben Software und jede Software ist fast wie ein Naturgesetz. Die hat Fehler. Die Technik, die hat Fehler und die Angreifer nutzen diese Fehler aus. In der Fachsprache nennt man das Vulnerabilities. Und ein Angreifer, der jetzt dann genau weiß, welche Software ich installiert

00:25:54 **Speaker 4**

habe und der weiß, welche Fehler die hat, der kann das ausnützen. Das ist ein großer Ansatz, dass wir einfach die Technik besser machen müssen und das Schlagwort wäre Sicherheit bei Design und zum Beispiel insofern, weil ich da auf das sehr stolz bin, weil das Technologie Hightech made in Austria ist, das weltweit funktioniert. Wir bauen zum Beispiel Werkzeuge, die bieten das an, die dem Entwickler, der dann IT-Systeme baut, von Anfang an mit schaut mit ihm, sozusagen wie eine, ist jetzt künstliche Intelligenz, aber wie ein Werkzeug und ihm im Vornherein sagt: Wenn du das so baust, dann wirst du da anfällig sein. Also ich kann hier Sicherheit schon von Anfang an, vom Gedenken der Architektur, wie baue ich das Auto, das digital fährt oder das Smartphone oder eine Kontrolleinrichtung oder eine App, dass die ja sicher ist. Das muss werden. Das Problem, warum wir das nicht tun, ist jetzt, kommen wir noch mal zurück, es ist nicht nur Bequemlichkeit. Das würde ich noch mal mit uns gerne teilen.

00:26:52 **Speaker 4**

Wir haben so wie immer, wenn es um Sicherheit geht, das Problem wir alle, auch Unternehmen, auch wir als Privatpersonen. Es hat am Anfang keinen Wert. Wir sind nicht bereit, dafür was zu zahlen. Das ist das Problem, das wir weltweit in der Industrie dann haben. Und wenn niemand dafür was zahlt, ja dann wird's nicht. Wir zahlen dafür, dass der Flieger nicht runterfällt. Darum ist das Flugzeug auch etwas teurer. Wenn man das so bauen würde, wie wir heute IT normal verkaufen, schnell eine App schreiben, reinstellen und alle verwenden es, dann würde jeder Flieger runterfallen. Das tun wir nicht. Und das Problem müssen wir noch in Griff kriegen. Sicherheit muss für uns alle einen Wert haben als Markt. Dann würden auch die Hersteller würden sie meinen Security by Design Ansatz machen, dass jene Unternehmen, die bestimmte Produkte bauen, die wirklich sicher sein müssen, sei es beim Kraftwerksbetreiber, sei es bei einem Roboter baut oder auch die, die Autos bauen, die nehmen das ernst. Alle anderen,

00:27:46 **Speaker 4**

die sagen, ich tue mal, ich will Geld verdienen, und stelle was rein, geben auf das nicht acht, weil dafür nichts bezahlt wird. Das ist eine Kunst. Und das diskutieren wir jetzt ganz massiv auch auf der Industrieseite. Das war der eine Bereich, also dass wir sichere Systeme bauen. Das zweite, was noch

wichtig ist, da kannst du sicher ergänzen aus der Sicht des IT- Betriebs. Nachdem wir die Technik haben, muss die auch betrieben werden. Da sitzen Menschen und schalten Software ein, aus, steuern ein Kraftwerk. Die brauchen jetzt aber auch laufende, jedes Jahr neue Ausbildung, weil sich die Technik laufend verändert. Sie müssen weitergebildet werden. Also im Gegensatz zur Hochschulausbildung, vier Jahre wäre ein guter Informatiker, müssen jetzt auch die, die im Kraftwerk sitzen, das Kraftwerk betreiben, die in der Steuerungsanlage, die in der Fabrik sind und Roboter betreiben, die müssen laufend weitergebildet werden. Und dafür bin ich auch stolz. Hier ist Österreich das erste und einzige

00:28:41 **Speaker 4**

durch das AIT offizielle Weiterbildungszentrum für die Atomenergiebehörde. Das heißt, unsere Experten und Expertinnen sind in der ganzen Welt und zeigen den Kraftwerksbetreibern durch Schulungen, praktische Schulungen, ein, zwei Wochen, das Neueste, auf das sie aufpassen müssen, damit in ihren Betrieben Angriffe verhindert werden, also die menschliche Komponente. Wenn sie moderne Technik haben, die schon besser gebaut ist, dann erreichen wir einen Zustand, wo die Systeme dann schon sicher sind, wo ich jetzt keine Angst habe. Nur im normalen Markt draußen haben wir diesen hohen Sicherheitsstandard nicht, der auch nicht bezahlt wird. Und darum diskutieren wir das und sind wir alle Opfer davon, weil wir eigentlich sehr einfache, salopp billige Technik verwenden.

00:29:27 **Speaker 2**

Ich muss also meine Theorie erweitern: Bequemlichkeit und Zahlungsbereitschaft und Sicherheit, die ist woanders zu Hause. Okay? Herr Steiner, Sie haben, hoffe ich und denke ich, beides am Start. Also Fachkräfte, die irgendwie sich damit auskennen und Technik. Ähm, Sie haben schon gesagt, die Universität muss verschiedene Prozesse und Bereiche zur Verfügung stellen und diese Kernprozesse gehören geschützt. Ähm, wie halten Sie sozusagen den Betrieb offen für, der dann vernetzt ist, wo Ausbildung passieren kann, wo steter Wandel ist? Was wird vielleicht auch in der AGZ besprochen? Welche technischen Lösungen versprechen Erfolg?

00:30:07 **Speaker 3**

Ich will noch mal vielleicht ganz kurz zurückkommen, sozusagen von der warum wir sozusagen als Universitäten in dieser Situation sind, wo wir jetzt sind, sozusagen, wo wir uns eigentlich zum Teil überfordert fühlen, sehr viele Angriffsvektoren haben, viele, viele verschiedene Facetten zu, zu lösen haben. Und das war sozusagen auch die Idee, vor einem Jahr ist die gegründet worden, sozusagen in Kooperation mit der UNIKO, dass wir als Universitäten uns in Kooperation anschauen müssen, wie

können wir diese riesige Flut an, an Angriffsvektoren und Möglichkeiten, äh, die, die da draußen im Internet passieren, gemeinsam lösen? Wir haben dann vor einen Jahr ein, ein großes Projekt initiiert. Das war das UVSEC-Projekt, das war das Vorprojekt, wo wir uns einmal sozusagen auditiert haben, sozusagen gegen, gegenüber den, äh, gegenüber einen externen Auditor und mal geschaut haben, wo stehen wir als Universitäten, äh, und wie stehen wir da und wo haben wir unsere Schwachstellen und, und wie können wir

00:31:12 **Speaker 3**

uns auch dagegen schützen? Und da haben alle zweiundzwanzig Universitäten sozusagen auch mitgemacht und, und sozusagen gemeinsam versucht, ihre, äh, IT-Security transparent darzustellen. Und das Ergebnis war vielleicht nicht das, was alle erwartet haben. Es gibt wirklich Universitäten, die sehr weit sind, Universitäten, die vielleicht weniger weit sind. Aber was uns das auf jeden Fall gegeben hat, ist sozusagen, wir, wir müssen gemeinsam einen Standard schaffen, wie wir sozusagen uns als Universitäten-und Ökosysteme, als Universität, äh, gegen diese Cybersecurity positionieren. Das hat dann auch sozusagen dazu geführt, dass wir genau drei Ebenen adressiert haben. Wir haben die, die Uniko, das ist sozusagen alle Vizerektoren, also Managementebene. Dann haben wir die Arge Cid, sozusagen die sehr stark operative Ebene, und wir haben die Arge Secure, die, äh, sozusagen die Fachspezialisten sind, mit einbezogen und haben gesagt: „Was müssen wir tun, sozusagen um das auf Schiene zu bekommen?"

00:32:18 **Speaker 3**

Und daraus hat sich sozusagen auch das, äh, diese Kooperation ergeben, dass wir, äh, mit dem Ministerium gemeinsam versucht haben, diese Kampagne und, und diese Cyber-Resilience-Thematik sozusagen gut zu adressieren, um sozusagen fit zu werden, um... Und das ist vielleicht auch ein großer Punkt, nachdem wir heute noch nicht adressiert haben... Es gibt ja sehr starke Regulatoriken, die auf Organisationen einwirken. Und diese Regulatoriken zwingen uns aber auch, sozusagen, äh, gewisse Standards und Prozesse innerhalb der Organisation und auch, äh, außerhalb der Organisation zu etablieren. Und die zur Etablierung sozusagen und diese Dings haben wir uns als, als Universitäten jetzt auch einen klaren Fahrplan gegeben, äh, der über die nächsten drei, drei Jahre passiert. Und was wir merken, sozusagen, dass wir uns auch als Orga-- Universitätshochlandschaft, sozusagen als Systempartner positionieren wollen. Wir wollen uns nicht nur, sozusagen als einzelne Universität, äh, an, an, an allen, in

00:33:24 **Speaker 3**

allen Bundesländern und, und, äh, in Österreich positionieren, sondern wirklich, wir brauchen Systempartnerschaft. Wir wollen sozusagen auch mit anderen Systempartnern kooperieren, nicht nur sozusagen innerhalb der Universität, sondern auch außerhalb. Und das ist, glaube ich, auch der Schlüssel am Ende des Tages zum Erfolg, dass man, wenn wir gute Kooperationen innerhalb der verschiedenen Organisationen und Stakeholdern schaffen, wir auch, äh, die Möglichkeit schaffen, sozusagen, uns auch gegen diesen, äh, schlechten Vibe, der sozusagen außerhalb, da, da ihren eigenen Markt und Industrie aufgebaut hat, uns klar zu positionieren und zu sagen: „Ja, wir haben Fehler und wir sind verwundbar, aber wir, wir haben mehrere Sicherheitsnetze, die uns davor schützen, dass sozusagen, äh, diese, dieser Angriffsvektor überhaupt realisierbar wird." Und das führt mir auch wieder dazu, sozusagen, dass man das am Ende des Tages den, den Benutzer oder die Benutzerin oder den Studierenden oder den, den Forschenden

00:34:28 **Speaker 3**

oder den, den Mitarbeiter oder Mitarbeiterinnen der Verwaltung in den Mittelpunkt setzen müssen. Wir müssen sozusagen die Leute dort abholen, wo sie sind. Dazu haben wir auch einige kooperative Projekte, sozusagen in unserem Gremium installiert. Das eine ist, sozusagen, wir wollen sozusagen gewisse Regulatoriken. free the bond practices heißt das. Das heißt, wir versuchen, einheitliche Sicherheitsrichtlinien über zweiundzwanzig Universitäten hinweg gemeinsam zu entwickeln und, und voranzutreiben. Das Zweite, was, was Sie vorher schon angesprochen haben, ist das Thema Awareness und Training. Das heißt, wir müssen unsere Studierenden, Mitarbeiter und Mitarbeiterinnen trainieren und auch, äh, die Awareness schaffen. Das erste Fangnetz sozusagen zu überwinden und zu sagen, wenn das ein Phishing Mail ist, dann, äh, kann ich, kann ich das sozusagen aufgrund gewissen I-Indikatoren erkennen und frühzeitig schon sozusagen, bevor ich draufklick, äh, löschen oder in den, in den Spam-Ordner verschieben.

00:35:30 **Speaker 3**

Das Dritte ist auch, wir wollen uns mit dem Thema Cybersecurity Operation Center auseinandersetzen. Das heißt, auch dort alle zweiundzwanzig Universitäten zu versuchen, äh... Wir sind ja permanent alle zweiundzwanzig Universitäten tagtäglich stündlich irgendwelchen Angriffen ausgesetzt. Und diese Angriffe sozusagen frühzeitig zu, zu visualisieren über alle zweiundzwanzig Universitäten hinweg, dass man die, die, äh, diese Vulnerabilities frühzeitig, äh, schließen kann, hilft natürlich sozusagen auch dem gegenüber. Und ein großes Thema ist natürlich einerseits die technischen Maßnahmen. Auch dort haben wir ein kooperatives Projekt. Das ist na-natürlich ein riesiges Portfolio, aber wir versuchen-Ähm, die Idee dahinter ist ja auch, sozusagen Services zu etablieren, die wir als Universität konsumieren können, äh, und auch dahingehend sozusagen

Synergien und, und Ressourcen effizient einzusetzen. Und das fünfte kooperative Projekt, das wir, äh, ähm, initiiert haben, ist, dass wir, äh, Sicherheitsüberprüfungen

00:36:35 **Speaker 3**

sozusagen, äh, machen. Das heißt, wir schauen uns an, welche, äh, wie schaut unsere Universität von außen aus, wie schaut die Universität von innen aus, welche Vulnerabilities haben wir? Wie können wir sozusagen standardisierte Tests in unseren Applikationen, die ja mannigfaltig sind, durchführen und sozusagen einen gewiss-- einen gewissen Grundschutz, äh, zu etablieren und die, die Mitarbeiter sozusagen noch, noch gar nicht sozusagen von diesen technologischen Themen, die da im Hintergrund ablaufen, ähm, zu informieren, sondern sozusagen ihnen das Werkzeug in die Hand zu geben, nämlich das, was sie gern tun und auch viel tun. Das ist, Leute, die in der Forschung sind, wollen natürlich forschen und wollen natürlich, äh, neue Technologien ausprobieren und da on the edge sein. Äh, Leute in der Verwaltung und, äh, Leute in der Lehre haben halt die Aufgabe, den, den, dem, den Studierenden Wissen gut und, und, und, und einfach zu vermitteln. Und ich glaube auch, dass es eine Grundausbildung

00:37:39 **Speaker 3**

braucht, sozusagen, wie wir zumindest Studierende im Bereich von Cybersecurity, äh, ausbilden, aber natürlich auch sozusagen das Wissen in dem Bereich auch heben. Und im Zuge dessen sind natürlich-- haben wir klar gesagt, wir haben eine klare Strategie für uns als Universitäten. Wir haben, wir wollen unsere, ähm, Informationssicherheit stärken. Wir wollen unsere, äh, Mitarbeiter ins Zentrum setzen. Wir wollen uns nachhaltig sozusagen auch dem, dem Thema widmen und wollen auch das Thema Kooperation in den Vordergrund setzen. Und nur so glaube ich, dass uns das am Ende des Tages über zweiundzwanzig Ökosysteme in Österreich gelingen wird.

00:38:25 **Speaker 2**

Okay, also Kooperation sozusagen als, als, ähm, ein starker Hebel, ähm, die, die Analyse und das, äh, sozusagen zu wissen, wo hakt es denn bei jedem Einzelnen, das auch wechselseitig transparent zu machen, das Know-how an den Universitäten auch nutzen, um neue Lösungen zu entwickeln. Das ist bei Ihnen alles schon passiert. Dann, ja, jetzt haben Sie sozusagen den User schon ins Zentrum hineingeholt, den Benutzer. Deswegen machen wir an dieser Stelle weiter. Äh, Frau Wimmerzahl, Sie haben's schon gesagt, Anwendungen sollen sicher sein und benutzbar bleiben. Hmm? Eine gesunde Skepsis der User:innen bleibt wie in allen Lebensbereichen auch im Cyberspace unbedingt notwendig. Also wenn wir jetzt sagen, die Technik ist zwar da, aber sie ist teilweise fast undurchschaubar, was würden Sie denn jetzt allen hier irgendwie mitgeben? Wie, wie schult man

diesen Muskel? Wie, ähm, was, was sollen wir sozusagen tun, damit wir uns vor Internetbetrug schützen? Wir selber nämlich. Technische Lösungen, das

00:39:30 **Speaker 2**

ist alles gut und schön. Wer den Nerv hat, die sieben Passkeys zu installieren, super. Aber was, was können wir, was können wir tun? Wir User und Userinnen, wir, das Problem vor dem Bildschirm.

00:39:43 **Speaker 5**

Ja, wir müssen uns, wie der Kollege schon gesagt hat, zuallererst von der Idee lösen, dass das Internet eine heile Welt ist, eine gute Welt ist, wo alles schön ist. Ähm, das stimmt schon lange nicht mehr. Ähm, und wir müssen sagen, das Internet ist ja auch nur ein Abbild der echten Welt. Also Dinge, die mir in der echten Welt passieren können, können wir auch im Internet passieren. Ähm, und in der echten Welt kann sich jemand als Polizist verkleiden und mich kontrollieren. Und auch da sollte ich skeptisch sein und, und sollte ich darauf achten, hat er eine Marke, äh, und so weiter und so fort. Und genau dasselbe trifft halt auch auf den Cyberspace zu. Auch dort sollte ich immer im Hinterkopf haben, ja, ist das jetzt authentisch? Ist das jetzt-- Könnte das jetzt wirklich sein? Ist das eine Nummer von... Hat, hat, hat mich diese Nummer schon mal angerufen oder nicht? Äh, von wo stammt diese Nummer? Gott sei Dank kann man österreichische Nummern nicht mehr gut spoofen. Das heißt, die stammen

00:40:37 **Speaker 5**

dann eh meistens aus dem Ausland. Dann muss ich schon mal skeptisch sein und sagen: Na ja, wen kenne ich in Deutschland oder in China oder in Frankreich oder wo die Nummer herkommt? Ähm, ist es plausibel, dass mich über diese Nummer jetzt meine verschollene Nichte anruft oder nicht? Habe ich eine verschollene Nichte? Das ist vielleicht der erste Punkt, aber gut, das, das weiß ich vielleicht doch. Ähm, also ich denke, genau dieselbe gesunde Skepsis, die ich im echten Leben habe, sollte ich einfach im Cyberspace auch haben.

00:41:09 **Speaker 2**

Aber was mache ich? Sie haben es nämlich vorhin auch schon ganz gezielt angesprochen. Eben, wir sind grad am Aufwachen, noch nicht ganz munter. Wir sind grad am Einschlafen, wir sind nicht mehr ganz von dieser Welt. Ähm, da wird ja sozusagen auch damit gearbeitet, Leute einfach unter Druck zu setzen, in Zugzwang zu bringen. Da muss schnell, da wird, äh, da werden irgendwelche aktuellen Dinge aufgegriffen, die dann natürlich, weil man das eh schon irgendwo gehört hat, noch mal

plausibler sind. Wie tue ich mit so was? Soll ich mir einfach für alles eine, weiß ich nicht, zumindest zehnminütige Bedenkfrist ausbitten und sagen: „Okay, durchatmen?"

00:41:46 **Speaker 5**

Das wär schon mal sehr klug. Das wär schon mal sehr klug. Ähm, und was ich auch sehr hilfreich fände, wäre eine zweite Meinung. Also sich nicht zu blöd zu sein und sagen, ja, da, da frag ich jetzt einmal meinen Partner, meine Freundin. Auch wenn das vielleicht ein heikles, sensibles Thema ist. Oft sind ja diese, äh, Mails auch mit kompromittierenden Themen. Da darf ich mir dann nicht zu schade sein und sagen, ja, ich hab' eine beste Freundin, einen besten Freund, ich hab' eine Mama, einen Papa, ich hab' eine Tochter, einen Sohn, äh, und die frag ich jetzt einmal. So viel Zeit muss sein. Also diese fünf Minuten, diese zehn Minuten oder diese Stunde nehme ich mir, bis ich jemanden erreicht habe und rede mal drüber. Und-Ähm, dann, wenn ich das bespreche, fallen mir vielleicht schon einige Seltsamheiten auf.

00:42:29 **Speaker 2**

Mhm, mhm, okay. Äh, Herr Leopold, Sie sagen, Cybersicherheit ist, ist eine Kulturfrage. Internetsicherheit kann jetzt per se nicht nur auf Technik ausgelagert werden oder in IT-Abteilungen ausgelagert werden oder den CIO ausgelagert werden, sondern sie muss irgendwie von allen zumindest ein bisschen verstanden werden. Die berufliche Weiterbildung haben Sie vorhin schon erwähnt, für die Leute, die damit zu tun haben, jetzt noch mal ausgenommen. Also Awareness von der Führung bis zu allen Mitarbeitern. Äh, brauchen alle Berufszweige eine Basisschulung? Wird das künftig so sein wie das ABC? Wir müssen das ABC einmal lernen und dann können wir uns hoffentlich den Rest unseres Lebens alle möglichen geschriebenen Inhalte zu Gemüte führen. Oder ist es mehr so wie, also Radfahren ist da nicht... Was, was müssen wir denn ständig neu lernen? Vielleicht das, was Sie jetzt gleich sagen werden.

00:43:19 **Speaker 4**

Sehr genau. Lassen Sie mich einen Satz davon noch mal sagen, weil man's, glaube ich, noch nicht so deutlich herausgestrichen hat-- haben bis dato. Warum ist das für uns eigentlich a wichtige Diskussion, für uns alle? Ich glaube, was heute anders ist wie die letzten vierzig Jahre, wenn wir begonnen haben, seitdem sich jetzt die Informatik, das Internet entwickelt hat, ähm, es gilt für jeden von uns, für jeden Unternehmer, für die Behörde, für uns als Staat, aber auch für uns als Privatperson: Wenn unsere IT-Plattform, nennen wir es jetzt mal Internet, schlampig, also unsere PCs, Smartphones und mit der, mit der Kommunikationsmöglichkeit nicht mehr vorhanden ist, können wir alle nicht mehr leben. Es gibt keine Steuererklärung, es gibt kein Gehalt, es-- Ich finde,

Sie können nicht aufs Amt geben. Und dann ist das auf der ganzen Welt so. Das ist ein Problem und das sind wir uns alle noch nicht so richtig bewusst geworden. Schon ein wenig. Darum gibt's jetzt auch sehr starke Anstrengungen, zum

00:44:19 **Speaker 4**

Beispiel seitens der Europäischen Kommission und der Mitgliedstaaten, dass wir hier neue Gesetze einführen, neue Regulierungen einführen, damit wir diese kritische Infrastruktur, das ist die-- Es gibt auch keinen Strom mehr, wenn die IT nicht funktioniert. Das hat sich schon umgedreht. Darum ist es für uns alle als gesellschaftlich wichtiges Thema, dessen wir uns annehmen müssen. Sonst könnte man sagen, das macht jetzt irgendeiner in der IT unten. Ja, das ist das Problem, das wir noch haben. Ich würde sagen, salopp, es gibt zwei Arten von Unternehmen: die, die das ernst nehmen und dann ist es eine Chefsache geworden und dann kostet's auch was, dann ist es Teil von dem Ganzen, ja; und welche, die immer noch sagen: „Nicht mein Problem, das macht mir irgendein Techniker." Und es ist kein Techniker-Problem alleine, es ist viel größer. Und wir gemeinsam auch noch mal, vielleicht ein kurzer Ausflug, warum gibt's denn diese Phishing-E-Mails da? Was will man da überhaupt? Na ja, wir sind alle ja

00:45:12 **Speaker 4**

auch Nutzer dieser Systeme. Wir sind Teil des Systems. Als Mitarbeiter bin ich irgendwo drin und benutze einen PC, vielleicht nicht in dem kritischen Bereich, aber es ist der erste, das erste Eintrittstor, dass ich in ein IT-System komme. Und jetzt wird's schon spooky auch, weil wir KI auch da oben gesprochen haben. Was wird jetzt anders? Na ja, jetzt werden wir beobachtet und darum wird's plötzlich schon interessant, wenn man auch sagen würde: Na, was sind meine Privatdaten? Was will mir da schon ein großer Angreifer? Wir werden immer mehr solche Mails bekommen, Nachrichten bekommen, die ziemlich ausgetüftelt sind und bei weitem nicht von Menschen, sondern von Maschinen, die genau wissen, was sie interessiert, was sie tun, und wenn sie ein ganz, ein seltenes Hobby haben. Und genau da wird ihnen jetzt ein super Angebot gemacht. Das kannst du haben, klick da drauf. Es wird immer ausgefeilter und wir klicken dann drauf und damit helfen wir mit, unser IT-System zu kompromittieren. Das heißt,

00:46:04 **Speaker 4**

jeder, jeder von uns ist Teil von dessen. Darum ist diese Awareness so wichtig und ich würde jetzt den Begriff einführen, wir brauchen so was wie ein kollektives Bewusstsein. Auch in dieser Technik brauchen wir eine, mir gefällt der Begriff, Cyberhygiene, ein Minimummaß im Umgang und nicht ein gedankenloses, nicht ein "Es ist mir wurscht". Ich hab-- Es ist ein Aufwand, es geht nicht anders. Es

kostet was und ist ein Aufwand. Das ist der Teil eins. Der Teil zwei ist dann natürlich, das ist dann mehr für die Profis und die Experten. Da müssen wir noch viel mehr tun. Da brauchen wir auch gute, ausgebildete junge Studenten, viel mehr noch, und Studentinnen, die sich auskennen, wie man solche Systeme dann echt baut, damit wir in der nächsten Generation viel bessere Systeme haben, die, wo die Technik in sich, sich selbst kontrolliert – kann man immer reden – oder die Technik by Design besser gemacht wird, Privatsphäre by Design, Sicherheit bei Design, damit uns als Benutzer dann diese Last genommen

00:46:59 **Speaker 4**

wird.

00:47:01 **Speaker 2**

Okay, also nicht nur die Fashion Victims da draußen sind vielleicht bedroht, sondern auch die Fans von Modelleisenbahnen. Wenn ihnen die Maschine das richtige Mehl zuspielt und sie klicken drauf, sind sie trotzdem. Ich glaube, ähm, also, die Tatsache, dass uns das alle was angeht, das sehen wir hier im Raum auch ganz gut. Es ist ziemlich voll. Ich glaube, hier sitzen ein paar Leute, die schon verstanden haben, dass uns das alle was angeht. Ich möchte jetzt noch, ähm, zwei Dinge kurz klären, bevor wir ins Publikum hineingehen. Und zwar schaue ich rüber zur Frau Wimmerzahl, weil mit mir gemeinsam erreichen wir am Podium Geschlechterparität. Ähm, ich bin allerdings in der Informatik nicht so gut wie sie und in der Informatik ist das auch noch nicht der Fall. Ähm, ich möchte kurz als kleinen Sidestep einfach, ähm, fragen: Wo muss Ihres Erachtens angesetzt werden, wenn wir eben viele Sicherheitsfachkräfte brauchen? Studenten, Studentinnen, wie Sie gesagt haben. Ähm, wo muss angesetzt werden,

00:47:57 **Speaker 2**

um dieses attraktive Berufsbild an Mädchen und an junge Frauen zu bringen? Und warum braucht es überhaupt mehr Frauen auch in der IT-Sicherheit?

00:48:04 **Speaker 5**

Mhm. Ja, die IT im, im Gesamten ist ja sehr männlich besetzt, immer noch. Ähm, und die Systeme sind daher sehr oft von Männern erdacht und, und gemacht. Ähm, ich denke, dass Frauen da schon auch einen anderen Blickwinkel darauf haben, ähm, und dass gerade die IT-Sicherheit ein sehr lohnenswertes Feld für Frauen ist und wir das-- Die Frage ist, wie kriegen wir die Frauen hierher? Ähm, wir gehen viel in die Schulen, holen die Schulen zu uns, ähm, und versuchen da auch, die Mädchen konkret anzusprechen, äh, und zu zeigen, was man bei uns alles lernen kann, ähm-Denn

der, der Job in der IT-Sicherheit ist ja ein sehr sinnstiftender Job. Man macht ja da, man ist auf der guten Seite. Also man kämpft gegen das Böse auf der guten Seite und das ist schon was, was auch Frauen sehr anspricht. Also gerade auch, auch Männer, aber auch Frauen sind auf der Suche nach Jobs, die einen Sinn machen, wo man etwas Gutes bewirkt, was für die Gesellschaft tut. Und da wäre die IT-Sicherheit eigentlich eine sehr,

00:49:05 **Speaker 5**

sehr große Spielwiese für genau diesen Sinn und ich glaube, das müssen wir noch mehr kommunizieren. Ähm, nicht nur das gute Gehalt danach, äh, und die tollen Jobchancen, sondern eben auch, auch diese sinnstiftende Tätigkeit, die man auf jeden Fall hat. Und es wird auch nie, nie langweilig. Also ich, ich denke, das wäre für alle ein interessanter Job, vielleicht auch für die Töchter und Söhne, die Sie zu uns schicken möchten. Ähm, die sind dann auch sehr gut ausgebildet und können auch Ihnen weiterhelfen, ja.

00:49:36 **Speaker 4**

Genau.

00:49:37 **Speaker 5**

Genau, nicht nur dem Unternehmen. Ähm, ja, und ich denke, da müssen wir einfach noch mehr das kommunizieren.

00:49:44 **Speaker 2**

Mhm. Also gehen Sie nach Hause zu Ihren Töchtern und Söhnen und sagen Sie Ihnen, ein, ein Job mit gutem Gehalt und mit Sinn. Dass sich Töchter und Söhne neben Erwachsene stellen, sobald die das Handy rausnehmen, ist für mich zu Hause ein sehr vertrauter Anblick. Da stellt man sich immer neben mich, weil es könnte sein, dass ich Unterstützung brauche. Gut, das dazu. Ähm, ich möchte noch eine Sache ansprechen, weil es, glaube ich, äh, einfach, äh, interessant ist und weil wir hier gleich zwei Leute sitzen haben, die beide Teil vom GAIA-X-Netzwerk der EU sind, das sich um Datensicherheit, Datennutzung und Datensouveränität bemüht. Ich glaube, es ist, ähm, man kann sagen, die EU versucht irgendwie ein bisschen einen eigenen Weg, äh, zu gehen, äh, und, äh, sich sozusagen hohe Standards zu geben in einigen Belangen, wo es um IT oder um KI oder andere technische Gegebenheiten geht. Ähm, können Sie kurz umreißen, wie, wie kümmert man sich dort um, um Datenschutzfragen und Datensouveränitätsfragen?

00:50:50 **Speaker 2**

Vielleicht macht einer Datenschutz, einer Datensouveränität?

00:50:54 **Speaker 4**

Ich fang mal an, ja.

00:50:56 **Speaker 2**

Er fängt einmal an, gut.

00:50:58 **Speaker 3**

Danke, dass sie das Thema auch aufwerfen, weil ich glaube, das ist durchaus ein, ein spannendes Thema, das es, das uns zukünftig vielleicht einiges an Kopfweh, äh, nehmen kann. Ähm, warum kommt dieses Thema überhaupt sozusagen von der Europäischen Union? Ich glaube, der Treiber dafür sind die Fülle an Regulatoriken, die auf Unternehmen zukommen, um die überhaupt zu bewältigen, quasi zueinander oder zwischeneinander Daten austauschen zu können. Das ist sehr domänenspezifisch auch. Wenn ich jetzt sozusagen im Education-Umfeld, äh, bleibe, wo, wo wir als Universität natürlich auch ein Glied sind, äh, dann, dann wollen wir sozusagen ja Daten zwischen verschiedenen Universitäten austauschen, wollen aber zugleich sozusagen nicht, äh, irgendwelche Datenschutzverletzungen machen, weil wenn wir von Universität A zu einer Universität B Daten transferieren, dann dürfen wir dies auch nicht ohne Zustimmung der jeweiligen Person machen und dergleichen. Und alle diese, diese Lösungen, die da sozusagen

00:52:03 **Speaker 3**

jetzt am Markt erst kommen, es gibt noch kein Patentrezept für diese, für diese Technologie, aber sie entstehen und man merkt sozusagen, es gibt einerseits die Möglichkeit, ich brauche ein vertrauenswürdiges Umfeld, wo ich verifizieren kann, dass die Entität oder die Organisation die Organisation ist, dass die Person die Person ist und dergleichen. Und alle diese Themen werden sozusagen in, in, in vielen EU-Staaten derzeit aufgebaut und dazu entsteht Infrastruktur. Äh, und diese Infrastruktur sozusagen kann man dann nutzen, um Personen zu verifizieren, um Institutionen zu verifizieren, um Daten zu verifizieren, weil man an ein Ministerium, äh, herantreten kann, sozusagen um gewisse Sachen abzufragen, ohne dass man gleich sozusagen irgendwelche Datenschutzverletzungen hat. Ähm, der Hintergrund: Es braucht ein vertrauenswürdiges Umfeld, das das sicherstellt, dass das auch passieren kann. Und diese Technologie wird gerade geschaffen. Man nennt das sozusagen dann Datenökosysteme oder Data Space

00:53:12 **Speaker 3**

sozusagen als Modewort, wo man sozusagen mit verschiedenen Konnektoren sozusagen unter gewissen Rahmenbedingungen Daten austauschen kann, Verträge abschließen kann und das alles im digitalen Raum.

00:53:27 **Speaker 2**

Okay.

00:53:27 **Speaker 3**

Und GAIA-X bietet sozusagen dazu Möglichkeiten, um ein vertrauenswürdiges Umfeld zu schaffen.

00:53:35 **Speaker 2**

Und was ist jetzt dann Datensouveränität?

00:53:38 **Speaker 4**

Da übernehme ich jetzt, genau. Also Souveränität... Wir haben jetzt vorher länger das Thema Cybersecurity behandelt, wo es darum geht, dass die technische Plattform, wo wir Daten abspeichern, übertragen, ausweisen, die verfügbar ist und nicht kompromittiert wird. Das ist eine. Die Diskussion ist darüber, was passiert mit unseren Daten? Kann jetzt unser Urlaubsfoto sein, kann eine Maschinensteuerungsdatenanleitung sein für einen Produzenten, äh, für ein, ein Unternehmen, der einen Roboter oder einen Automaten in seinem Fabrik benutzt. Ähm, kann ein Text sein, dass Sie schreiben... Sind unsere Daten. Ähm, was ist sozusagen jetzt passiert? Ich glaube, ist allgemein bekannt, was gerade die Zeitalter der künstlichen Intelligenz, die diversen großen Angebote wie ChatGPT. Warum funktioniert das so super? Es ist ganz, im Wesentlichen ganz einfach. Sind halt große Computer, mag schon sein, aber es wurden alle Texte, die in der Welt die letzten Jahrzehnte geschrieben wurden, einfach verwendet und

00:54:39 **Speaker 4**

einem Computer gefüttert, sozusagen. Es hat sich niemand drum gekümmert, wem die Daten gehört. Das wird jede Menge von IPR-Verletzungen, die Rechteverletzungen, Privatsphäre... Das ist alles dahinter und dort haben wir eine coole Maschine. Wir haben uns alle gedacht, äh, und keiner hat uns gefragt. Keiner hat euch gefragt. Es wurde einfach verwendet.Warum ist das so? Wir haben heute noch das Problem, dass über siebzig Prozent der Daten oder an die siebzig Prozent der Daten in der Europäischen Union, also von uns allen, von hundert Millionen Menschen, die Daten produzieren, Unternehmen und Privatsphäre, die liegen auf irgendwelchen Servern, die von ganz wenigen Unternehmen, sechs an der Zahl, alle sechs sind amerikanische Unternehmen, die auf denen ihren Servern liegen. Wir haben keine Möglichkeit zu kontrollieren, was die mit den Daten

tun. Das geht nicht. Die liegen irgendwo draußen, dort gibt es ja Gesetze in anderen Ländern, die dürfen das sogar nach ihren Gesetzen. Wir haben als Österreich,

00:55:31 **Speaker 4**

als EU keine Chance, da irgendwie einen Anspruch zu erheben. Es ist einfach, die Daten können missbraucht werden, sie können analysiert werden, man kann KI-Systeme gebaut werden, sie können gegen uns verwendet werden. Das ist verlorene Souveränität. Dann zu einem Ansatz funktioniert keine Wirtschaft mehr, weil Souveränität brauchst du, um in einer Wirtschaft agieren zu können. Und aus meiner Sicht noch viel schlimmer, so funktioniert auch keine Demokratie mehr. Wenn wir nicht mehr selber entscheiden können, was wir tun, sind unsere Staaten aufgelöst. Das ist jetzt das Problem, das der Europäische Union jetzt angeht und sagt, so kann es nicht weitergehen. Wir bauen jetzt ein System ein und am Schluss brauchen wir das, damit jeder von uns, der seine Daten hat, meine Daten sind meine, mein Foto ist meins, mein Text ist meins, dass ich bestimmen kann. Ich habe die Freiheit, ich gebe sie jetzt diesem Unternehmen, ich verkaufe sie, wenn ich sie will, ich gebe sie jemandem, aber mit Bedingungen.

00:56:23 **Speaker 4**

Du darfst sie nur dazu verwenden und das technische System, nennen wir es wieder Internet, meine Computer, die passen darauf auf. Damit ist ausgeschlossen, wenn ich jetzt jemandem meine E-Mail schicke, der darf sie dann nur einmal verwenden und einmal lesen und kein mal nicht mehr kopieren und weiterschicken. So kann man sich das vorstellen. Wenn wir das nicht schaffen in der Welt, dann haben wir ein sehr beträchtliches Problem, weil dieses, die Datenhoheit am Schluss unser Leben, unsere Wirtschaft, aber auch unsere Gesellschaft bestimmt. Darum ist das nicht nur eine, wie Sie gesagt haben, die EU geht andere Wege. Am Schluss wird es die ganze Welt brauchen, weil das die Grundlage ist, dass wir als vernünftige Gesellschaften miteinander leben können und nicht ganz wenigen Akteuren, Monopolbetrieben ausgeliefert sind.

00:57:09 **Speaker 2**

Mhm. Ich glaube, heute hat einer dieser Monopolbetriebe ein kleines Flackern in seinen Serverfarmen. Deswegen haben heute ein paar Dinge nicht funktioniert und hier hat es auch gerade kurz geflackert. Ähm, okay, gut. Datensouveränität haben wir das auch besprochen. Ich möchte, ich drehe mich jetzt zu Ihnen. Sie haben sich vielleicht schon allerhand Dinge gefragt. Da ist schon eine Hand oben. Bitte oben lassen. Okay, eins, zwei, drei, oje, vier, fünf, sechs. Okay, gut. Wir merken uns das und wenn die Frage gestellt ist, vielleicht sammeln wir in diesem Quadranten da drüben die Fragen zusammen. Los geht's.

00:57:48 **Speaker 6**

Ah, ich bin schon dran, ja. Ah, Frage Thema Deepfake. Da wurde bis jetzt sehr wenig gesagt. Ähm, das Thema ist brandgefährlich, auch demokratiepolitisch, weil die Meinungen von Menschen kommen stark aus Bildern. Und wenn ich jetzt nicht mehr weiß, wo die herkommen, klar. Konkrete Fragen, ähm, gibt es für einen Normalverbraucher, technisch interessiert wie mich zum Beispiel, gibt es eine Möglichkeit, Deepfakes zu identifizieren? Also komme ich irgendwie vernünftig an Software heran, die mir sagen kann, ob ein Bild künstlich ist oder nicht? Und, äh, gibt es eine Kennzeichnungspflicht für Deepfakes? Also ob Bilder echt sind oder künstlich.

00:58:38 **Speaker 2**

Okay, wollen wir die zweite Frage, die da in dem, auf der Seite war, auch noch reinholen einfach? Und dann arbeiten wir uns hier hinüber, wenn das geht. Bitte helfen Sie mit, genau einfach das Mikro weitergeben. Danke.

00:58:50 **Speaker 7**

Danke schön. Grüß Gott. Ah, erste Bemerkung, Gerhard Riemer, lange Zeit Industriellenvereinigung Bildung, Innovation, Forschung, auch ein bisschen in Brüssel. Erster Punkt. Danke vielmals, dass es möglich war, in dieser Qualität Persönlichkeiten und Kenntnisse aus verschiedenen Bereichen so zu bündeln, dass es wirklich spannend war. Ich konzentriere mich jetzt Gott sei Dank nur auf den letzten Bereich, das Internationale und das Europäische. Warum, ja?

00:59:19 **Speaker 4**

Ah, wenn wir die Weltentwicklung uns anschauen, dann rennt Europa, ah, oder die USA ja voran mit einem Präsidenten – da brauche ich dazu ja gar nichts sagen – der auch die Top-Universitäten da drüben versucht in den Griff zu bekommen. Leopold hat angedeutet, dass vieles von dort kommt, dass wenige Unternehmen, überwiegend aus den Amer-- aus den Vereinigten Staaten, die Hand drauf haben auf vieles. Und jetzt frage ich mich, und das ist der europäische Aspekt: Ich danke auch für die Hinweise dieser Vernetzung auf europäischer Ebene. Aber oder und: Reicht unsere Geschwindigkeit, etwas Seriöses aufzubauen, das von Anfang an gemeinsam in dem komplizierten Europa mit unterschiedlichen Ländern und Kulturen etwas hinzukriegen, um von den anderen nicht endgültig geschluckt zu werden. Wenn man jetzt die, die, das Verfahren im Rahmen der Vereinigten Staaten sich anschaut, alles, was bremst, die Technologie, wird beseitigt oder reduziert. Wir in Europa bemühen uns auch im Sinne der Demokratie, die

01:00:26 **Speaker 4**

Dinge möglichst seriös, möglichst, ah, auch zur Erhaltung der Demokratie ordentlich zu machen, verantwortungsbewusst zu machen.

01:00:34 **Speaker 2**

Also sind wir schnell genug? So, kann man das so- -fassen . Ja. Also sind wir schnell genug? Gibt es eine Deepfake-Identifikationsmöglichkeit für technisch versierte, interessierte Privatpersonen und gibt es eine Kennzeichnungspflicht für Deepfake? Wer mag antworten?

01:00:54 **Speaker 8**

Fang an.

01:00:56 **Speaker 5**

Vielleicht fange ich mal aus technischer Sicht an, wobei Deepfakes jetzt nicht mein Spezialgebiet sind. Ähm, mein Spezialgebiet ist die Authentifizierung und mein Punkt ist wieder: Wenn wir nur authentifizierte Anrufe annehmen würden, hätten wir kein Problem. Also wenn wir nur Anrufe von Nummern annehmen, die in meinem Adressbuch sind, habe ich das Problem gar nicht, dass ich einen Deepfake erkennen muss, weil dann sind es nur meine Kontakte. Ähm, wenn ich das Internet aber so nutzen möchte, dass mich jeder anrufen kann, dann erst habe ich das Problem mit dem Deepfake und dann muss ich mir überlegen, ähm, ja, kann ich das erkennen? Ob es da jetzt schon freie Tools gibt, bin i, bin i überfragt, müsste man recherchieren. Es gibt diese allgemeinen Tipps, dass man darauf achten kann. Gibt es Artefakte im Bild, gerade da, wo der Kopf sozusagen endet, gerade bei den Haaren und so weiter, äh, gerade bei den Bewegungen. Da gibt es ja schon Tipps und Hinweise, auf was man achten kann, weil viele

01:01:47 **Speaker 5**

Deepfakes noch nicht so gut gemacht sind, dass man sie net auch mit dem bloßen Auge erkennen kann. Erster Punkt. Zweiter Punkt: Es gibt sicher KI-gestützte Lösungen, die das auch wieder erkennen können, aber ob's da was gratis gibt für den Endanwender, das, Endanwenderin, weiß ich jetzt nicht. Ähm, aber mein Punkt ist halt eigentlich, wir sollten schon mal skeptisch sein, wenn wir einen Anruf von einer Nummer kriegen, die wir nicht kennen oder von einer ausländischen Nummer kriegen. Und dann sollte man net einfach blauäugig glauben, ja, das ist der Tom Cruise, der mich da anruft. Ähm, das muss ich halt dann hinterfragen, vielleicht wieder wen Zweiten dazuholen und, und, und bitten, mir da, mir da zu helfen. Ähm, ja, also ich denke, mit Authentifizierung davor wäre das gelöst. Im Unternehmenskontext sehe ich da auch kein großes Problem. Die, äh, großen, äh,

Videokonferenzplattformen haben Authentifizierung dabei. Ähm, das heißt, meine Gesprächspartner, die in dem Call sind, die, die sind

01:02:35 **Speaker 5**

schon authentifiziert. Äh, da muss ich mir um Deepfakes auch keine Sorgen machen. Also es geht wieder die gesunde Skepsis meiner Meinung nach.

01:02:42 **Speaker 8**

Okay, Kennzeichnung wahrscheinlich nicht, sonst wäre ja die ganze Deepfake-Sache völlig ad absurdum geführt. Da muss ich ja nichts mehr faken, wenn ich alles kennzeichne.

01:02:51 **Speaker 3**

Ich würde es aus so einer, aus so einer operativen Ebene sozusagen das Thema Deepfake kurz betrachten, weil es uns einfach auch tagtäglich betrifft an Universitäten. Ähm, ganz klar sozusagen, Universitäten sozusagen ist ja auch sozusagen, wo Wissen generiert oder neues Wissen generiert wird. Ähm, und um das auch sozusagen machen zu können, braucht es natürlich sozusagen Bibliotheken, Wissen, wo bestehendes Wissen vorhanden ist. Und was passiert, ist natürlich sozusagen, man nutzt natürlich den einfachen Weg, sozusagen über diese Modelle, die da weltweit, sozusagen wie die, wie die Schwammerl aus dem Boden schießen, äh, zu nutzen. Und ich mache es weder an Studierenden, ähm, nehme es übel, sozusagen, dass er diese Informationsquelle, die ist ja nichts anderes ist wie eine Informationsquelle, ähm, nutzt und, und versucht, sozusagen, äh, da auch sozusagen bestmöglich durch das Studium zu kommen. Ähm, das heißt, auch da werden wir sozusagen, und das Bild ist natürlich vielleicht nur sinnbildlich

01:03:56 **Speaker 3**

gesprochen, äh, ein Problem. Ich glaube, wir brauchen eine klare Regelung, wie wir AI-generierte Inhalte kennzeichnen und, äh, auch nachvollziehbar machen, wie sie generiert worden sind, sprich, wie sie gepromptet werden und solche Sachen. Also da gibt es sehr, äh, gibt's einige Methoden, die sich jetzt sozusagen noch nicht standardisiert haben, aber man merkt auch sozusagen, dass sich da was tut. Ähm, aber von dem her, ich glaube, wir müssen sozusagen durchaus immer diese kritische Skepsis mit, mit in uns tragen, sozusagen. Äh, kann das, was da steht, mit Referenzen und, äh, ja auch Verlinkungen nachvollziehbar überprüft werden. Und das ist sozusagen, glaube ich, auch das, was am Ende des Tages das wissenschaftliche Arbeiten ausmacht, dass wir Informationen, die wir generieren oder neu generieren und eine kritische Frage dazu stellen, eine These auch sozusagen

irgendwie belegen oder widerlegen können. Das, glaube ich, gilt's halt langfristig auch zu adressieren. Und das zweite Thema, vielleicht

01:05:08 **Speaker 3**

noch zum Thema, äh, Internationalisierung und Geschwindigkeit. Reicht das aus für uns, äh, in dem Bereich? Hmmm, ich glaube, man sollte die Kirche im Dorf lassen. Ähm, man kann immer kritisieren, dass wir zu langsam sind, aber ich glaube, es braucht diesen Prozess in der Gesellschaft, dass wir, ähm, das, was gerade passiert, auch die Menschen mitnehmen können. Ich glaube, das ist ein essentielles Thema, dass wenn wir nach, nach Amerika schauen, wo wir, äh, einen Häuptling haben, der vorausreitet, Äh, und nicht auf die Menschen achtet, dann passiert genau das Gegenteil, dass wir skeptisch sind, dass die Leute sich auflehnen und alle diese Themen, die wir hier sehen. Und das, glaube ich, braucht eine gewisse Zeit, um auch zu verstehen, wie können wir diese Geschwindigkeit, die derzeit natürlich durch verschiedene Modelle auch vorgegeben wird, standhalten. Und da glaube ich, sind wir nicht so schlecht in Europa.

01:06:16 **Speaker 8**

Darf ich da ergänzen? Also zum Ersten: Deepfake, äh, Prophezeiung. Wenn das so weitergeht, wird keiner mehr von uns das Internet verwenden, weil alles gefaked ist und dann macht's keinen Spaß mehr. Man wird einfach die echten Sachen kennzeichnen müssen. Habe ich auch schon gehört.

01:06:33 **Speaker 3**

Genau, Alternativen haben. Also ich glaube an das. So kann's nicht weitergehen. Macht keinen Sinn. Ohne Geld, das kostet gar nichts. Es ist alles verfügbar im Internet. Es braucht keinerlei Ausbildung, man braucht nicht studieren gehen. Acht Milliarden Menschen haben die Macht, beliebig Filme, die früher Kinofilme mit Riesenetats gemacht haben. Es wird alles... Es ist faszinierend, aber es wird nur noch gefaked draußen. Also-

01:06:59 **Speaker 4**

Ähm, das heißt, es ist sehr wichtig, dass wir das Thema angreifen. Das ist richtig. Außerdem sollten wir es als Gesellschaft angehen. Es beginnt auch langsam. Da mache ich vielleicht eine kurze Eigenwerbung. Es beginnt langsam. Also die erste Community ist eigentlich die Medienbranche, die aus meiner Sicht sehr gut darauf anspringt. Es geht um das Thema Faktchecking. Ich muss ja wissen: Woher kommen die Bilder? Die Texte, Stimmen, die sind ja vorne, also sind die erfunden worden? Hier, die, ähm, die APA gemeinsam mit der Deutschen Presser Agentur, France Press Agency haben ja unter dem Titel „Gartmore", eine europäische Initiative, German Austrian Digital Media

Observatory, wo genau ein großeuropäisches Projekt, das ist das zweite schon, wo genau diese Frage geklärt wird: Wie können wir gemeinsam Fact-Checking besser machen, auch Daten austauschen? Dann auch ein Thema. Und darunter moderne Werkzeuge verwenden, die mir Deepfakes oder Fakes erklären, ob das jetzt Bilder sind, Bewegtbilder,

01:07:52 **Speaker 4**

aber auch Text und da die Zusammenhänge. Also die große Forschung in den Initiativen, die Schwerpunkte gehen genau in die Richtung, diese Zusammenhänge im Internet zu verstehen. Kann es sein, dass dieser Artikel richtig ist? Ist die Quelle richtig? Das ist ja alles so viel geworden, das können Menschen nicht mehr fassen. Hier brauchen wir Werkzeuge. Solche Werkzeuge werden auch in Österreich gebaut. Da bin ich sehr stolz. Wir haben vor zehn Jahren damit begonnen am OIT, in meinem Team, und wir sind einer der führenden Technologieanbieter, zum Beispiel für der, äh, GARTMORE-Initiative, wo wir solche Werkzeuge, äh, bauen, damit, äh, der Analyst solche Änderungen von Inhalten rasch erkennen kann. Ohne Werkzeuge wird das nicht mehr gehen.

01:08:33 **Speaker 2**

Aber sie kosten.

01:08:35 **Speaker 4**

Moment, ja. Es kommt auf die Frage hin. Ähm, na ja, der Aufwand ist da, macht das Sinn. Aber nichtsdestotrotz, ich würde jetzt mal frech die Frage beantworten wird jetzt auf Ihre Frage: Gibt es das halt für jeden? Nein, gibt es noch nicht. Ich bin der Meinung, das muss es geben. Das gehört zu zum ABC in Zukunft. Ich muss lesen können, ich muss sinnerfassend lesen können und in Zukunft brauchen wir alle ein Minimum an Werkzeug, ein Hilfsmittel, ein Minimum. Das ist sozusagen, ja, ein Minimum. Es ist nicht jeder ein Super-- von uns ein Super-Literat, aber ein Minimum, dass ich meine Plausi-Checks machen kann und das Werkzeug muss mir helfen, sonst werden wir das Internet nicht mehr verwenden können. Und das muss gratis für alle sein, wäre meine persönliche Meinung. Für alle, sonst wird das Internet keinen Mehrwert haben. Für die professionelle Nutzung dann, ob es dann jetzt im, im Medienbereich sind oder im Behördenbereich. Es gibt Gesetze mittlerweile. Der AI Act fordert ja gerade so etwas,

01:09:29 **Speaker 4**

dass der, der eine KI verwendet und einen Inhalt verändert, muss es kennzeichnen. Aber natürlich braucht man dann wieder Kompetenzen: Wie kann ich das überprüfen, wenn es einer nicht tut? Und damit sind wir wieder bei diesem Wettrüsten: Ich brauche Kompetenzen, ich brauche Werkzeuge.

Da müssen wir viel mehr tun. Das passt aber zur zweiten Frage: Na ja, warum haben wir den Zustand? Weil bisher alles gratis war. Easy. Hat jeder alles verwendet und es war egal. Nein, es ist ein Aufwand wieder. Wir brauchen Werkzeuge dafür. Ähm, darum auf die Frage, Gerhard, wie das mit der EU ist. Ich glaube, am Schluss, ich hab, ich glaube an das Gute im Menschen, wenn uns bewusst wird, dass das, was wir verwenden, wirklich funktioniert und dass es sicher ist und dass ich nicht ein gefaktes irgendwas bekomme, sondern das funktioniert, dann braucht es Anbieter, die so was anbieten, die vielleicht ein Gütesiegel haben, das ich kontrollieren kann und wo ich dann als Konsument auch bereit bin. Das ist ein Mehrwert

01:10:26 **Speaker 4**

für mich. Alles gratis kann nicht funktionieren. Irgendwie muss man dafür zahlen. Dann werden wir auch eine bessere, wieder funktionierende Internetinformationsaustauschmaschine haben. Zurzeit haben wir es nicht.

01:10:37 **Speaker 2**

Okay, das wäre fast schon ein schönes Schlusswort, aber wir hatten noch sehr viele Fragen und deswegen würde ich bitten, dass jetzt einmal der mittlere Sektor, was da für Fragen waren. Genau eins, zwei, drei, vier. Und dann waren, glaube ich, noch zwei da drüben. Ähm, ja, da mal in der ersten Reihe, genau. Bitte keine Co-Kommentare, knappe Frage und dann bitte knappe Antwort. Danke. So, erste Reihe.

01:11:01 **Speaker 9**

Da das alles nun ziemlich kryptisch geklungen hat, stellt sich mir die Frage: Ist es sinnvoll, eine VPN anzulegen? Zum Ersten. Zum Zweiten finde ich die große Gefahr der Cookies, denn das Internet funktioniert ja wirtschaftlich und wenn die Cookies dann wieder zurückkommen als irgendein Inserat oder ein Kauf oder eine Möglichkeit, etwas zu bestellen, dann ist es ja sinnvoll, das Cookie wegzuschalten, bevor ich das Internet einschalte und nachher die Löschfunktion einzuleiten. Aber das geht natürlich nicht, denn dann komme ich ja gar nicht auf die, auf die Frage oder auf die, auf die Essenz dessen, was ich im Internet erreichen will. Also muss ich sie immer eingeschalten lassen. Ist das nicht irgendwo ein großes Handicap?

01:11:46 **Speaker 2**

Okay, also VPN und Cookies. Dann, äh, hinten noch eine Frage.

01:11:50 **Speaker 10**

Ja, hallo erst mal und vielen Dank erst mal für Ihre Ausführungen. Mir scheint, dass es einige Akteure gibt im Internet, die gar kein Interesse haben, dass es sicherer wird. Ich denke da an, ähm, Marketingbuden oder, ähm, große soziale Netzwerke, die vielleicht, ähm, ja, was man da-- als Beispiel, aber auch vor allem staatliche Akteure, die, äh, eben gerne Hintertüren in sicheren Messengern einbauen wollen. Und auf der anderen Seite gibt es sehr starkes Desinteresse in manchen Bereichen, dort sicheres Internet zur Verfügung zu stellen oder überhaupt sichere Infrastruktur. Da denke ich an Schulen, ähm, Spitäler, ähm, auch Ämter noch. Ähm, wie, wie sehen Sie das? Und wenn Sie mir da zustimmen, ähm, was wären die Strategien dagegen oder do-tätig zu werden? Danke schön.

01:12:45 **Speaker 2**

Okay.

01:12:47 **Speaker 3**

Soll ich anfangen? Ganz kurz?

01:12:49 **Speaker 2**

Ja, ganz kurz.

01:12:50 **Speaker 4**

Kurze Antwort. Also VPN-Frage: Ja, natürlich. Bei uns im Unternehmen, kein Mitarbeiter darf einsteigen von seinem Smartphone oder von seinem PC äh-Um auf unsere Server zu gelangen, weil er kein VPN verwendet. Ja, natürlich, geht nicht, weil sonst hören alle anderen mit. Also ist ja klar, ein Muss. Ah, auf das Thema Cookies, aber passt auch auf diese allgemeine Frage. Zwei Sätze zur Erklärung, wo Sie vorher gesagt haben, vor vierzig Jahren haben wir begonnen. Ah, wir haben begonnen und das Internet ist begleitet worden mit dem Thema alle gleich und wir benutzen was gemeinsam und es kostet nichts. Ähm, ich war das selber Zeitzeuge. Es hat in meiner ganzen Zeit damals, die ersten zwanzig Jahren, in Europa niemand verstanden, dass die größten Geschäftsmodelle, das ist das, warum jetzt Facebook funktioniert, Google funktioniert, äh, die ganzen Social Media funktionieren. Da ist kein unmittelbares, direktes Geschäftsmodell. Einer verkauft jemandem was. Es ist Werbung dahinter. Punkt. Wir erliegen

01:13:49 **Speaker 4**

alle da Werbung. Es ist nicht gratis. Wir zahlen mit Aufmerksamkeit. Das ist ein Thema für mich, für die Bildung. Wir müssen die Kinder dazu bekommen, dass sie in Zukunft merken, Werbung ist auch ein Wert draufschauen. Das heißt, es wird dann besser, wenn wir verstehen, gemeinsam, das ist ein

gesellschaftliches Diskurs, den wir machen müssen. Es ist nicht gratis. Und dann kann, und wenn's dann Anbieter gibt, am Schluss muss es der freie Markt sein. Wenn's Anbieter gibt, die mir was Vernünftiges anbieten und ich als vernünftiger Konsument entscheiden kann, heut kann ich nicht, weil es gibt nur ganz wenige, das ist das Problem, dann wird sich der Markt auch aussortieren. Und wenn ich dann bewusst weiß, wann zahle ich als Werbekunde und wann zahle ich als Bezahlkunde? Das sind im Prinzip zurzeit die zwei großen Geschäftsmodelle. Und darum haben die Werben, Werbeanbieter, ah, Betreiber kein Interesse daran, dass die Cookies verschwinden. Die wollen die natürlich, um uns zu beobachten. Klar,

01:14:39 **Speaker 4**

da sind wir mitten drin. Wir sind am Umbau des Internets, was uns die nächsten zehn, zwanzig Jahre beschäftigen wird.

01:14:44 **Speaker 2**

Also wir zahlen immer mit Aufmerksamkeit, mit Daten. Ja, Frau Wimer-Zell?

01:14:48 **Speaker 5**

Ich möchte zu den Cookies vielleicht noch kurz ergänzen. Das ist wieder jetzt eine Sache zwischen Security und Benutzbarkeit. Natürlich ist es praktisch, wenn ich das nächste Mal, wenn ich die Seite aufrufe, schon wieder eingeloggt bin und mir nicht noch mal mein Passwort eingeben muss. Das macht auch das Cookie. Also, das Cookie hat auch Vorteile für mich, für die Benutzbarkeit. Umgekehrt natürlich kann man immer alle Cookies löschen. Das hat jetzt keinen großen Nachteil, außer dass ich mich immer überall wieder anmelden muss. Also, das seh ich überhaupt kein Problem, weil das ja die konkrete Frage war, soll ich meine Cookies löschen? Jederzeit. Und zum Thema VPN vielleicht, ja, ist sicher keine, keine schlechte Idee. Ähm, für den Privatnutzer, die Privatnutzerin hat es den Effekt, dass ich eine sichere Verbindung zu einem externen Server aufbauen. Von dort gehen dann meine Anfragen los. Das heißt, alle Dienste, die ich aufrufe, sehen als IP-Quelladresse nur mehr diesen externen Server

01:15:34 **Speaker 5**

und nicht mich. Also, das gibt mir mehr Privatsphäre natürlich, ah, und es hat vielleicht den positiven Nebeneffekt, dass ich, wenn ich eine VPN in Deutschland zum Beispiel habe, dass ich dann auch deutsche Mediatheken nutzen kann, zum Beispiel, wo wir ein Geoblocking haben. Genau, auch dafür wird VPN gern genutzt.

01:15:50 **Speaker 2**

Vielleicht, wenn wir hier schon gerade ein bisschen auch in dem kleinteiligeren Bereich sitzen. Was mache ich jetzt konkret? VPN, ja, nein, Cookies, ja, nein und so. Ähm, gab's eine Frage vorab, die, äh, jemand im Stream, äh, gestellt hat. Jemand, der in mehreren Projekten global im Internet unterwegs ist und derzeit glücklicherweise keine Probleme mit Hacking hat, sich aber für die Zukunft absichern und Fehlern vermeiden möchte. Momentan wird sichtlich ein Virenschutzprogramm, äh, genützt. Ähm, er fühlt sich damit oder sie fühlt sich damit gut geschützt. Ist das gerechtfertigt? Oder sollten wir das jetzt, also alles, was heute schon besprochen wird, auf jeden Fall auch, quasi, wäre die Empfehlung?

01:16:34 **Speaker 5**

Genau. Je mehr, desto gut. Also, ein Antivirenprogramm schützt mich vor Viren, zumindest vor bekannten Viren, vielleicht auch vor unbekannten, das weiß ich jetzt nicht. Ich kenn das Produkt nicht. Ähm, aber es schützt mich nicht vor einem Phishing-Angriff. Kann es nicht, wenn es ein Antivirenprogramm ist. Insofern, ja...

01:16:50 **Speaker 2**

Ich hoffe, der oder die User:in hat schon die ganze Zeit gut aufgepasst, was alles schon gesagt wurde. So, wir sind immer noch in diesem mittleren Sektor. Eins, zwei, drei und dann gehen wir in diesen drüberen Sektor, sonst ist es ungerecht. Versuchen wir alle drei Fragen. Lassen Sie die Hand oben, dass wir sie sehen können. So, da und da. Okay. Bitte. Kurze Frage, kurze Antwort.

01:17:11 **Speaker 11**

Cyberhygiene wurde genannt und eigentlich jeder Österreicher, jede Österreicherin sollte grundlegende Fähigkeiten haben. Jetzt hatte in Österreich vor ein paar Jahren eine Projektentwicklung des Staatssekretariats gegeben, digitale Fitness für jeden Österreicher. Und in diesen Checks und Testfragen waren viele sehr ausgefeilte Cyber-Security-Fragen drinnen, die nicht ohne waren, und KI-Fragen drinnen. Und irgendwo habe ich den Eindruck, das Produkt ist nicht weitergegangen, es ist eingestellt worden, keine Ahnung was, aber es wäre damals ein super Turbo gewesen und die Frage ist ja, es hätte die Antworten auf viele der heutigen gestellten Fragen gegeben. Und das zweite ist, diese Themen werden in der Schule behandelt, unter anderem in der digitalen Grundbildung, die aber mit einer Stunde per Woche bei den Zehn- bis Vierzehnjährigen natürlich überfordert ist. Einerseits von der Qualifikation der Lehrenden, die eigentlich viel besser vernetzt gehörten und gebrieft werden müssten für diese

01:18:14 **Speaker 11**

Themenstellungen. Also wäre ein Lösungsansatz, das eigentlich fast in Richtung Hauptfach auszuwerten. Danke.

01:18:22 **Speaker 2**

Das waren eigentlich keine Fragen, aber wir nehmen es mit. Gut, Anregungen. Ja, der Herr im weißen Pullover.

01:18:30 **Speaker 4**

Ja, da-danke. Ähm, zum, zu Anfang danke schön für den sehr interessanten Talk. Äh, ich hab' wirklich eine kurze Frage. Äh, ihr habt gesprochen über die KI-Ansätze für Cyberangriffe und, äh, Deepfakes und Phishing. Aber gibt es schon KI-Einsätze zu Bekämpfung von, äh, Betrügern, also Betrugs-, ah, Betrugsbekämpfung?

01:18:51 **Speaker 2**

Okay, geben Sie das Mikro gleich vorne zu dem Herrn zwei Reihen weiter vorne und wir nehmen die Frage noch mit.

01:18:57 **Speaker 5**

Steininger, Steininger Consulting. Ich hätte eine-

01:19:01 **Speaker 12**

Äh, Frage: Wie werden diese EU-Vorschriften kontrolliert, exekutiert? Denn ich hatte ein Erlebnis, eine Plattform, in der ich seit Jahren bin, hat einen, einen Bildschirm gebracht, äh, weil's, äh, aufgrund der, äh, Sicherheitsbe- oder einer sie-- äh, es-europäischen Gesetzeslage müssen wir, äh, fragen, ob wir die Daten weitergehen können an das, den ganzen Konzern. Die Seite hatte keine Möglichkeit zum Ablehnen, hatte nur des, des Weiter-- nicht einmal weiter, sondern los geht's. Und meiner Meinung widerspricht es der Datenschutzgrundverordnung und das habe ich der österreichischen Datenschutzgrundverordnung, äh, -organisation geschickt. Äh, die haben mir geantwortet nach, äh, zwei Wochen, äh, gut wischiwaschi: „Wenn es Ihnen nicht gefällt, dann klagen Sie die, das internationale Konzern." Und, äh, da finde ich, müsste, äh, da-das von der, äh, exekutiert werden, dass man so etwas nicht, äh, lässt, denn da öffnet man Tür und Tor für weitere Funktionen.

01:20:28 **Speaker 2**

Okay, ich bin nicht sicher, ob wir das hier lösen können, aber es ist sicher noch nicht perfekt. Wie sieht es aus mit KI im Einsatz für das Gute? So habe ich das jetzt mal mitgenommen.

01:20:38 **Speaker 4**

Also wenn ich da an... Willst du anfangen?

01:20:39 **Speaker 5**

Ähm, ich kann gern anfangen. Ähm, also ja, KI kann man für viel Gutes auch einsetzen. Natürlich, es gibt schon Tools, um Deepfakes zu erkennen. Ja, auch KI-gestützte Tools. Wir an unserem Department, äh, verwenden KI, ähm, auch für das Gute. Ähm, zum Beispiel in der Verarbeitung von großen Datenmengen, zum Beispiel, ähm, in der Objekterkennung in Livestreams, dass man gefährliche Objekte erkennt, ähm, auf Überwachungskameras oder auf Drohnenvideos, live in Echtzeit. Ähm, da haben wir Projekte gehabt. Äh, wir verwenden KI auch für die forensische Analyse. Auch da gibt es große Datenmengen. Wann schon was passiert ist, sozusagen, dann muss man ja aufarbeiten, was ist passiert und da kann die KI wunderbar helfen. Also die KI kann große Datenmengen, Videodaten analysieren und sagen: Wo kommt welcher Gegenstand, welche Person vor? Äh, große Audiodaten analysieren und sagen: Über welche Themen wird in diesem Audiofile gesprochen oder in welchen Audiofiles wird über interessante, für den Forensiker

01:21:39 **Speaker 5**

interessante Themen gesprochen und so weiter und so fort. Also die KI rein zu verteufeln, ist, ist, ist keine gute Idee, weil man kann mit der KI ganz viele gute Dinge auch machen, gerade bei der Verarbeitung von großen Datenmengen. Da ist sie ungeschlagen, ehrlich gesagt.

01:21:53 **Speaker 3**

Ich würde auch vielleicht kurz auf das antworten, weil das ist unser tagtägliches Doing, sozusagen, dass wir vielleicht nicht jetzt KI per se, aber zumindest, äh, Machine Learning. Wir haben hunderttausend Datenquellen und verschiedene Fangnetze, sozusagen, die uns gewisse Sensoren bieten, die wir im Netzwerk haben, auch Personen sind sozusagen solche Sensoren, äh, und die müssen zusammengeführt werden an, an einem Punkt, damit wir frühzeitig, sozusagen, erkennen: Ist das jetzt tatsächlich ein Angriff oder ist das jetzt, sozusagen, eine Normalität oder eine Abweichung der Normalität, weil ein Professor, sozusagen, irgendwelche Daten mit irgendjemandem in China austauschen will, äh, und dadurch, sozusagen, die Load von verschiedenen Systemen nach oben geht. Und diese Systeme, sozusagen, auf den verschiedenen Fangnetzen zu analysieren, zu identifizieren: Ist das jetzt ein Angriff oder ist das ein Normalverhalten? Das heißt, das ist unser tägliches Doing in, in Universitäten. Damit... Und

01:22:55 **Speaker 3**

das könnten nicht Menschen machen, sozusagen. Also das ist... Das wäre... Wenn man das heute in der heutigen Zeit noch glauben würde, sozusagen, die Menge an Daten, die wir da stündlich oder minütlich verarbeiten, sind nicht von Menschen bewältigbar. Das heißt, das müssen Maschinen am Ende des Tages machen, auswerten und analysieren. Und, äh, da hilft uns jetzt Machine Learning. KI kommt nach und nach rein. Also auch das ist kritisch zu hinterfragen: Was tun wir da in unsere Systeme rein? Wie gut funktionieren so KI-Systeme auch? Äh, aber auch dort braucht es a Skepsis und, und, und eine gewisse, einen gewissen Gegenpol, um das zu erreichen. Ähm, und zu dem Thema, äh, Kontrolle, äh, ich glaube, man sieht's ja einerseits auch an der NIS-zwei-Verordnung, ähm, dass auf europäischer Ebene diese Regulatoriken entstehen, dann in, in nationales Recht umzuwandeln sind und da ist natürlich jede, jede Nation für sich selbst auch zuständig.

01:23:57 **Speaker 2**

Was ist NIS zwei?

01:23:58 **Speaker 3**

NIS zwei ist die neue Verordnung, die, äh, ausgegeben wurde von der Regulatory Committee, um, äh, Cybersicherheits-, ähm...

01:24:08 **Speaker 4**

Sie haben's schon gekappt. Infrastrukturbetreiber.

01:24:10 **Speaker 3**

Infrastrukturbetreiber geht. Es hat die NIS eins gegeben und jetzt ist die NIS zwei Verordnung da, äh, die sozusagen... Bei der NIS-eins-Verordnung sind die Unternehmen aktiv vom, von dem Ministerium informiert worden. Bei NIS zwei gibt's a relativ klare Tabelle, wo man identifizieren kann, ob jetzt das Unternehmen, äh, in die NIS-zwei-Verordnung reinfällt und deshalb folgt keine aktive, äh, Informierung, sondern jedes Unternehmen muss sich, sozusagen, aufgrund dieser Prüfkriterien festlegen: Bin ich jetzt NIS-zwei-pflichtig oder nicht?

01:24:42 **Speaker 2**

Okay, also es wird kon-- es wird kontrolliert und es wird weiterentwickelt und es scheint sich, es scheint einfach ein besonderes Pech gewesen zu sein. Ergänzung, letzte.

01:24:51 **Speaker 4**

Ja, also das nur unterstreichend. Ähm, wir haben vorher über Hygiene gesprochen. Das ist normal für uns. Mehr brauchen wir nicht. Die, die jetzt wirklich für höhere Sicherheit, ob das jetzt die

Kraftwerksbetreiber, die vorher gesagt haben, die kritischen Infrastrukturbetreiber, ja, natürlich machen die eine Stufe weiter und die lassen ihre IT-Systeme durch KI, wie du es gesagt hast, überwachen.Und wir suchen... Und die Maschinen suchen Anomalien. Und das ist Stand der Technik. Braucht man für die nächste Generation. Auf die Frage, wie, ähm, äh, zu dir: Ähm, RTR ist hier die erste Stelle, wo man solche Beschwerden einbringt. Es gibt eine Schlichtungsstelle, äh, wo man sich über Unternehmen beschweren kann, die dann auch mit der Kommission gemeinsam den EU-Raum mit allen Regulierungsbehörden schon mittlerweile jetzt ein System aufspannen, um diesen Fehllauf, den es ja gibt von schlechten Anbietern, die sich nicht an Regeln halten. Darum gibt es auch die Gesetze. Also es beginnt schon langsam,

01:25:47 **Speaker 4**

ähm, das... Wir brauchen Kompetenzen dann auch dafür. Werkzeuge, ähm, Behörden, die die Werkzeuge verwenden, Unternehmen. Wir sind da relativ neu, aber das, ähm, entwickelt schon langsam. Was haben wir noch gehabt zum Thema Fit for Internet? Fit for Internet einerseits für die Jugendlichen und für die, sagen wir mal, normale Bevölkerung. Und das Zweite, die Ausbildungsinitiative, die ich vorher genannt habe, die wir machen für die, als obere Segment, Weiterbildung, die berufliche. Das verkaufen wir zurzeit gerade unter dem Titel, äh, Best Practice Austria International. Auf der ganzen Welt ist das, ähm, ein Angebot, das wir nach draußen bringen, was die ganze Welt hat. Einerseits für die Berufswelt, High End, und andererseits für die normalen Benutzer bis hin in die Schulen und natürlich in die Schulen, unterstreiche ich, da müssen wir noch viel mehr tun, um in der Bildung, sozusagen nicht nur Kompetenz, sondern Bildung: Was ist denn das Internet? Wie gehen wir mit den Daten um? Von klein

01:26:42 **Speaker 4**

auf in unserer Gesellschaft noch mehr verbreitern müssen. Da ist was zu tun, was wir gemeinsam zu tun haben.

01:26:47 **Speaker 2**

So, ich soll hier in vier Minuten die Veranstaltung beenden. Ich nehme jetzt noch eine Frage aus diesem Quadranten, damit da auch noch eine Frage gestellt werden kann, sofern sie noch offen ist. Hui, die sitzen direkt nebeneinander. Ich hoffe, Sie haben dieselbe Frage. So, da kommt das Mikro. Ganz flott.

01:27:07 **Speaker 13**

Wie macht man Online-Banking sicher? Benutzername und Passwort, das sechsstellig, es reicht schon lange nicht mehr.

01:27:16 **Speaker 2**

Okay, berechtigte Frage. Nebenan in Rosa.

01:27:20 **Speaker 5**

Ja, also vielleicht zusätzlich: Wie schützen sich die Banken vor solchen Angriffen- -und in weiterer Folge ihre Kunden?

01:27:27 **Speaker 2**

Wer kann zum Thema Banken was sagen?

01:27:29 **Speaker 4**

Also in aller Kürze: Wir haben das NIS-Gesetz angesprochen. Das ist ein Gesetz, das mittlerweile in jedem Mitgliedstaat gilt für kritische Infrastrukturbetreiber, Kraftwerksbetreiber, Fabriken. Und das Gleiche gibt es eigens nur für Banken. Die Banken haben auch mittlerweile EU-weit ein Gesetz, heißt DORA, wo hier ein großer Aufwand betrieben werden muss, um laufend nachzuweisen, wie man die IT-Infrastruktur sauber macht. Und das geht einher mit der Frage: Passwort und Username ist schon lange nicht mehr Stand der Technik. Das ist höchst unsicher. Steigen sie alle um auf Zwei-Faktor-Äh-Authentifizierung. Das heißt, Sie haben ein Gerät, Sie haben ein Passwort und nur wenn man beides gemeinsam hat, dann ist man noch mal eine Spur sicher. Abschlusssicher ist es immer nie. Es geht immer Risikomanagement, aber da sind wir mitten drin und auf ganz Österreich langsam umzusteigen. Das müssen wir tun.

01:28:19 **Speaker 2**

Okay, gut. Ich, ähm, mache jetzt keine Abschlussrunde angesichts der fortgeschrittenen Zeit, aber ich bedanke mich sehr, sehr herzlich bei meinem Podium, das alles gemacht hat von Highflyer, Kraftwerksbetreiber, wie wir können die Security by Design haben, bis zu Zwei-Faktor-Authentifizierung für alle. Also es war für jeden was dabei, glaube ich. Ähm, ich soll ein Resümee machen. Was soll ich Ihnen sagen? Bleiben Sie skeptisch, bleiben Sie dran, machen Sie das Internet wieder zu dem schönen, offenen, äh, informativen, lustigen Ort, als der es einmal gedacht war. Äh, der nächste Science Talk, kommen Sie bitte nicht hierher, 2026, gebe ich Ihnen mit, sondern an die TU Wien. Und wenn Sie am 26.10. noch nichts vorhaben, es ist der Tag der offenen Tür im Palais Dietrichstein, äh, im Ministerium mit Science Show, mit Wissenschaft erleben, Forschung entdecken,

Frauen stärken. Ähm, genau, zwischen zwölf und siebzehn Uhr. Das wäre die nächste Veranstaltung, wo Sie mit, äh, Science in Berührung kommen

01:29:30 **Speaker 2**

können. Ich bedanke mich bei Ihnen. Sie waren ein fantastisches Publikum. Sie waren ein fantastisches Podium. Ich wünsche uns allen noch einen schönen Abend und ein schönes, lustiges, offenes, sicheres Internet. Danke.