ZE
VE
DI

Digitalgespräch Folge 69

Lehren und Erfahrungen aus dem Cyber-Angriff auf die Uni Gießen

Mit Matthias Stenke von der Justus-Liebig-Universität Gießen, 16. September 2025
https://zevedi.de/digitalgespraech-069-matthias-stenke/

[Der Vorspann mit Musik und Ausschnitten aus dem Gespräch beginnt.]

Marlene Görger [mg]: Herr Stenke, Sie haben die stellvertretende Leitung und operative Leitung der IT-Sicherheit an der Justus-Liebig-Universität Gießen inne. Als die Uni 2019 diesen schweren IT-Angriff erlebte, waren Sie mittendrin.

Dr. Matthias Stenke [Stenke]: Die Uni war dann zunächst mal komplett offline. Also das war jetzt auch kein Vorfall, den man hätte, wirklich unter den Teppich kehren können. So nach dem Motto war es nur eine Abteilung oder so betroffen, die komplette Uni war digital tot. Ja, das macht sofort Schlagzeilen. Man hat da schon drauf geachtet seitens der Angreifer. Möglichst spät aufzufallen. Weil wenn das Mailsystem nicht geht, das ist, so das Erste, was dann auffällt. Die Stimmung war meines Erachtens von so einem großen Zusammenhalt geprägt. Wir sind angegriffen worden. Wir müssen jetzt sehen, wie wir damit umgehen. Also wir haben auch Kehrpakete bekommen.

[pgg]: Hat der Fall Gießen auch den anderen Hochschulen geholfen, sich einzustellen, umzustellen? Sind sie auch von anderen Hochschulen kontaktiert worden?

[Stenke] Die Bedrohungslage nimmt nicht ab, die nimmt eher zu. Und man muss da mehr machen, als man es vielleicht vor 10 Jahren gemacht hat.

[Der Vorspann endet, das Gespräch beginnt.]

[mg]: Die Abwehr von Cyberattacken. Heute ist der Alltag in Rechenzentren öffentlicher Einrichtungen. Die IT-Systeme sind permanent kleinen und größeren Angriffsversuchen ausgesetzt. Administratorinnen warnen Nutzen ihrer Systeme regelmäßig vor neuen Hackingmaschen oder verdächtigen E-Mails und informieren über kurzfristige Ausfälle. Öffentliche Aufmerksamkeit erhalten nur die großen und vor allem schmerzhaft erfolgreichen Angriffe. Längst ist allen klar, die Verantwortung für komplexe IT-Systeme tragen, der Vorfall im eigenen Haus wird eines Tages kommen. Wichtig ist es also, darauf gut vorbereitet zu sein. In Deutschland traf einer der ersten bekannt gewordenen Großangriffe auf eine öffentliche Einrichtung, die Justus-Liebig-Universität Gießen. Am 8. Dezember 2019 wurde eine Ransomware-Attacke auf die Systeme der Hochschule entdeckt und die ganze Universität sofort vom Internet getrennt. Was darauf folgte, war eine über Wochen und Monate andauernde Herkules-Aufgabe. Die Folgen des Angriffs blieben noch lange spürbar, das öffentliche Interesse war international riesig, die Unterstützung und Solidarität breit. Bis heute sind die Erfahrungen dieser Zeit wertvoll für die Verbesserung der IT-Sicherheit, nicht nur an Lehr- und Forschungseinrichtungen. Wie die Uni Gießen diese IT-Katastrophe erfolgreich bewältigte, welche Konsequenzen gezogen wurden, was andere öffentliche Einrichtungen lernen konnten und was man sich heute als Normalität in Sachen Cybersicherheit klar machen muss, darüber reden wir heute im Digitalgespräch. Mein Name ist Marlene Görger, ich bin Physikerin und Technikphilosophin und arbeite für das Zentrum verantwortungsbewusste Digitalisierung.

[pgg]: Und mein Name ist Petra Gehring. Ich bin Professorin für Philosophie an der Technischen Universität Darmstadt. Bei uns ist heute im virtuellen Podcaststudio Dr. Matthias Stenke aus Gießen zugeschaltet. Herzlich willkommen im Digitalgespräch, Herr Stenke. Wir sind sehr gespannt auf das, was Sie berichten.

[Stenke] Ja, ich freue mich, dass ich hier dabei sein darf.

[mg]: Herr Stenke, Sie haben die stellvertretende Leitung und operative Leitung der IT-Sicherheit an der Justus-Liebig-Universität Gießen inne und leiten zudem die Startstelle für Enterprise Architecture Management der Hochschule. Als die Uni Gießen 2019 diesen schweren IT-Angriff erlebte, der auch international für Aufsehen sorgte, waren Sie mittendrin. Wir erfahren von Ihnen also aus erster Hand, wie es ist, mit einer solchen Krisensituation konfrontiert zu sein, was zu tun ist und was Sie und Ihre Kollegen für Erkenntnisse gewonnen haben. Erzählen Sie uns doch bitte zum Einstieg. Was war an diesem Sonntagnachmittag im Dezember passiert?

[Stenke] Ja, an diesem Sonntag, das war ein Adventssonntag, meine Tochter hatte Geburtstag. Wir haben uns gerade auf die nachmittäglichen Feierlichkeiten vorbereitet. Hat sich ein Administrator aus der Veterinärmedizin bei uns gemeldet, bei unserer Rufbereitschaft vom Hochschulrechenzentrum und hat berichtet, dass einer der Server von einer Ransomware befallen sei. Aufgefallen ist es dadurch, dass die Mitarbeiter in der Veterinärklinik ihr Patientenverwaltungssystem nicht mehr benutzen konnten. Die Veterinärklinik arbeitet auch am Sonntag. Auf die Art und Weise ist das eben aufgefallen. Wir haben dann den Server vom Netz trennen lassen. Der Server ist hier im Hochschulrechenzentrum in unseren Serverräumen untergebracht. Deswegen war unsere Rufbereitschaft gefordert, dem Kollegen dann Zugang zu verschaffen. Und begleitend haben wir eben geprüft, ob noch weitere Auffälligkeiten bestehen. Das war auch der Fall. Wir haben dann festgestellt, dass weitere Systeme betroffen sind, auch von der gleichen Ransomware. Dann haben wir alle maßgeblichen Kolleginnen und Kollegen zusammengerufen, weitere Überprüfungen gemacht. Und dann hat sich eben herausgestellt, dass es ein großflächiger Angriff ist, von dem unsere Windows-Domain-Controller, also sozusagen die zentralen Steuerrechner, die für die komplette Windows-Infrastruktur zuständig sind, von diesem Angriff betroffen sind. Und wir haben auch festgestellt, dass die Angreifer sozusagen noch aktiv auf dem System waren. Wir haben zu dem Zeitpunkt am Sonntagmittag festgestellt, dass die Angreifer noch tätig waren und ihre Schadsoftware ausgebracht haben. Und dann haben wir relativ schnell die Entscheidung getroffen, in Rücksprache mit dem Präsidium die komplette Uni vom Netz zu nehmen, um den Angreifern eben die weiteren Möglichkeiten zu nehmen. Und alle Systeme runterzufahren, um die Schadensauswirkungen zu verringern. Was wir auch gesehen haben, war, dass die Verschlüsselungstrojaner, die ausgebracht worden sind, zum Teil noch nicht aktiv waren auf dem System, aber drauf waren, zum Teil gelaufen sind. Und da ging es eben darum, möglichst schnell die Systeme, die tatsächlich oder potenziell betroffen sind, runterzufahren. Um weitere Auswirkungen des Schadens zumindest zu verringern. Das waren die hauptsächlichen Aktivitäten im Laufe des Sonntags, an dem Sonntagnachmittag und im Endergebnis war Sonntagabend um 18 Uhr ungefähr die komplette IT der Uni runtergefahren. Also alle zentralen Serversysteme, nicht nur die Windows-basierten Systeme, sondern auch alle anderen, alle Linux-basierten Systeme, Speichersysteme, Netzwerk. Das heißt, die Uni war dann zunächst mal komplett offline. Am Abend gab es dann auch die erste Sitzung mit einem Krisenstab, der gebildet wurde. Um eben über die weiteren Schritte zu entscheiden, werden natürlich die Aufsichtsbehörden informiert. Das HMWK,

Hessisches Ministerium für Wissenschaft und Kunst, ist informiert worden. Der IT-Sicherheitsbereich im Innenministerium und so weiter als die vorgesehenen Meldewege des NKA ist eingeschaltet worden. Und im Ergebnis der ersten Krisensitzung. Gabs dann auch eine Information an die Öffentlichkeit noch am Sonntagabend über die sozialen Medien.

[pgg]: Ich frage kurz nochmal nach, so eine Universität ist ja eine super verzweigte Angelegenheit. Sie haben das jetzt eben angedeutet. Also es war tatsächlich betroffen, nicht nur so ein Fachbereich jetzt, die Veterinärmedizin oder Abteilungen der Universität, in denen sozusagen die Fächer sitzen, die unterrichten und forschen, sondern es war auch die Verwaltung sozusagen das zentrale Rückgrat betroffen.

[Stenke] Also tatsächlich betroffen von dem Vorfall, von dem Angriff selbst, von dem Verschlüsselungstrojaner war nicht alles. Aber wir haben eben aus Sicherheitsgründen erst mal alles runtergefahren und stillgelegt. Das heißt, es war wirklich alles komplett offline. Es ging kein WLAN mehr in sämtlichen Bereichen. Man kam von einem Arbeitsplatzrechner in einem Institut oder auch in der Verwaltung nicht mehr ins Internet. Es gab keinen Zugriff auf Dateiablagen, Zentrale, auf Netzlaufwerken. Es ging nichts mehr. Also wir waren… Digital komplett tot, kann man sagen. Das Einzige, was noch ging, war die Telefonanlage, die Telefonie, weil die eben noch nicht über Voice-over-IP oder solche Dienste lief, sondern zum damaligen Zeitpunkt noch eine klassische Telefonanlage war mit einer eigenen Infrastruktur. Das hat noch funktioniert, aber alle anderen Kommunikationsmittel und Dienste nicht mehr.

[pgg]: Und dann musste man das quasi Schritt für Schritt klären, wo ist der Befall?

[Stenke] genau, also in so einer Situation sind sie ja nur okay, ich habe hier einen großflächigen Angriff. Es sind viele Systeme betroffen. Aber man hat in den ersten Stunden noch nicht das komplette Bild. Und deswegen war der Ansatz, wir fahren alles runter, wir schalten ab, informieren. Das war eine der ersten Aktionen. Dann am Sonntagabend ging eine Meldung an Social Media raus. Wir hatten auch keine Kommunikationsmittel mehr. Wir hatten keine funktionierende Uni-Webseite. Das stand alles nicht mehr zur Verfügung. Der einzelne Kommunikationsweg waren öffentliche Kommunikationsmedien. Und da ist eben über Social Media informiert worden unter diesem Hashtag JLU-Offline. Und am nächsten Morgen ging es dann eben weiter mit den weiteren Analysen, auch mit externer Unterstützung. Weil in so einer Situation, das können Sie nicht allein. Da braucht man professionelle externe Unterstützung, die auf sowas auch ausgerichtet sind. Wir hatten Unterstützung von der Firma ER&W aus Heidelberg und wir hatten Unterstützung von Athene von dem Cyber-Security Forschungszentrum in Darmstadt. Und in der weiteren Analyse hat sich dann gezeigt, beim Prüfen der Systeme, dass die Windows-Infrastruktur betroffen ist. Die sogenannten Domain-Controller, also diese Steuerrechner der Windows-Domäne, waren befallen. Die wurden verwendet oder gekapert, übernommen von den Angreifern. Mit dem Ziel, von dort aus die Verschlüsselungstrojaner auszubringen auf alle Systeme, die im Netzwerk erreichbar waren. Und das waren zu dem Zeitpunkt natürlich alle Windows-basierten Server-Systeme, die in dieser Windows-Domainer integriert waren, aber auch eine Reihe von Endgeräten. Also auch am Wochenende läuft der eine oder andere PC noch in einem Labor oder in einem Büro, weil er nicht runtergefahren worden ist. Und die waren dann auch potenzielles Ziel für diese Verschlüsselungstrojaner. Das heißt die hier. Komplette Windows-basierte IT-Infrastruktur war entweder direkt betroffen, weil ein Verschlüsselungs-Trojaner da

schon losgelaufen war oder er war auf das System ausgebracht und ist noch nicht losgelaufen, weil dieses Loslaufen, das Starten, wurde in verschiedenen Wellen gemacht, so ein bisschen gestaffelt. Offenbar mit dem Ziel, nicht die ganze Infrastruktur komplett unter Volllast zu bringen, sondern das über einen gewissen Zeitraum ablaufen zu lassen. Aber das war da so der Stand, beispielsweise das Mail-System, was wir haben, basierend auf Microsoft Exchange. Da wurden zwei von den vier Servern, die wir zum damaligen Zeitpunkt hatten, komplett verschlüsselt und unbrauchbar gemacht. Aber zwei weitere wurden zwar auch kompromittiert, aber nur so weit, dass der Dienst selbst noch lief. Also man hat da schon drauf geachtet, seitens der Angreifer möglichst spät aufzufallen. Weil wenn das Mailsystem nicht geht, das ist, so das Erste aus meiner Erfahrung in jeder Organisation, was dann auffällt. Und das lief halt noch, das konnten wir auch benutzen. Aber es war kompromittiert. Es wurde auch versucht, die Datensicherung von den Systemen gezielt anzugreifen und unbrauchbar zu machen. Solche Versuche haben wir auch gesehen, teils erfolgreich, teils nicht erfolgreich. Aber Ziel des Angriffs war es, wie es in vielen anderen Fällen auch war. Diese Microsoft Windows-basierte Infrastruktur. Bei den Prüfungen später hat sich dann herausgestellt, wir haben ja auch dann die Linux-basierten Systeme und so weiter prüfen müssen. Bei dieser Prüfung hat sich dann herausgestellt, dass die Systeme nicht betroffen waren von dem Angriff, aber trotzdem mussten die eben überprüft werden, weil wir ja nicht wussten, was eventuell noch alles passiert sein könnte.

[pgg]: Und Ziel des Angriffs war Zerstörung oder Erpressung?

[Stenke] Sicherlich. Erpressung, uns hat aber keine konkrete löse Geldforderung erreicht, was wahrscheinlich auch damit zu tun hat, dass wir noch während der Angriff lief, am Sonntag runtergefahren haben, die Internetanbindung gekappt haben und dadurch natürlich auch schlecht erreichbar waren, maximal noch per Fax. Und das ist wahrscheinlich für solche kriminellen Angreiferbanden jetzt kein übliches Kommunikationsmedium. Und die Faxnummer wäre auch schwer herauszufinden gewesen, weil die Webseite auch offline war. Also wahrscheinlich ist deswegen da nichts angekommen. Aber das war das übliche Muster damals, diese Schadsoftware-Trojaner mit dem Ziel ich verschlüssle die Daten, um dann Lösegeld zu erpressen, gegen das dann der Entschlüsselungsschlüssel wieder ausgehändigt wird.

[mg]: Heißt das, sie haben den Angriff dann auch früh bemerkt?

[Stenke] Also wir haben es zumindest zu einem Zeitpunkt gemerkt, als noch nicht alles verschlüsselt war. Der eigentliche Angriff oder so die heiße Phase, wenn man das so nennen möchte, die begann am Freitagabend. Also nach Dienstschluss des meisten Personals, nach Dienstschluss der Administratoren. Am Freitagabend fand diese Übernahme dieser Windows-Domain-Controller statt. Also da haben die Angreifer den letzten Schritt gemacht und haben mithilfe von einem Kompromittierten. Account, Zugangsdaten mit administrativen Rechten, mit privilegierten Rechten, diesen Domain Controller übernommen und haben dann angefangen, von dort aus weiterzuarbeiten. Also beispielsweise wurde die Datensicherungskonfiguration vom Exchange System, also von dem Mail System versucht, so umzustellen, dass die Datensicherung unbrauchbar werden über das Wochenende. Das ist aber nicht gelungen. Auch der Angriffsversuch auf das Speichersystem, wo diese Datensicherungen liegen, ist nicht gelungen. Aber man hat in den Protokollen dieses Systems dann Versuche gesehen. Oder dann in der Nacht von Samstag auf Sonntag wurden die Exchange-Server dann kompromittiert. Also es lief so am Wochenende ab und das Ausprägen des

Verschlüsselungs-Trojaner, das passierte so auch in der Nacht von Samstag auf Sonntag ab 1.20 Uhr. Wenn ich es richtig in Erinnerung habe, da lief diese Verschlüsselung los. Und wir haben es dann eben am späten Vormittag bemerkt. Und wir konnten dann die Maßnahmen ergreifen und in die Schadensanalyse gehen.

[pgg]: Sie haben das jetzt schon angedeutet, da bricht natürlich eine riesige Kommunikationswelle los. Erstmal die ganzen Betroffenen und dann wahrscheinlich auch diejenigen, die versuchen, irgendwas zu managen oder zu helfen. Und die Öffentlichkeit. Wie organisiert man sowas? Hat die Uni da in der Schublade einen Plan liegen, wie man damit umgeht?

[Stenke] Das hatten wir damals tatsächlich noch nicht. Also zwischenzeitlich sind wir da besser aufgestellt. Aber das Krisenmanagement hat trotzdem aus meiner Sicht gut funktioniert, denn zentrale Stelle war so der Krisenstab des Präsidiums. Da waren die Präsidiumsmitglieder Bestandteil des Krisenstabs. Der Präsident hatte die Leitung. Es war die HZ-Leitung mit dabei. Ich war mit dabei. Die Leitung, Rechtsabteilung, Personal, Studium und Lehre. Also diese ganzen zentralen Bereiche. Präsidialbüro und auch die Pressestelle oder Kommunikation, Öffentlichkeitsarbeit war da immer dabei. Und dieser Krisenstab hat sich am Anfang täglich getroffen. Und da wurde eben immer geschaut, wie ist die Lage, was sind die nächsten Schritte? Und ganz wichtiger Punkt dabei war dann halt auch, was wird jetzt kommuniziert an wen? Gleich am Ende von diesen Sitzungen wurde dann eben festgelegt, was kommuniziert wird, über welchen Informationskanal. Am Anfang war das… Eine Notfall-Webseite, die wir am folgenden Montag bei der Uni Marburg online nehmen konnten. Das war so das erste Kommunikationsmittel, auch öffentlich zugänglich. Ja, also die Kommunikation richtete sich dann praktisch an alle, an die Mitarbeitenden, an die Studierenden, aber auch an die Öffentlichkeit, im Zweifelsfall auch an die Angreifer, die uns da unter Beschuss genommen hatten. Deswegen musste man da vorsichtig sein. Was man da kommuniziert. Aber das war immer ein integraler Bestandteil dieser Krisenstabssitzungen. Wie macht man die Kommunikation? Was muss an wen kommuniziert werden? Und wir hatten aber auch noch andere Gremien in dem Kontext. Es gab beispielsweise dann ab Januar 2020 eine sogenannte Notstandskoordination. Das war so eine Art erweiterter Krisenstab. Wo dann auch die Leitung der Fachbereiche, die Dekane und Dekane mit dabei war, die Leitung der Verwaltungsabteilung, die Leitung anderer zentraler Einrichtung, die Prüfungsämter, im Prinzip das komplette Führungs- und Leitungspersonal der Universität, um mit denen eben die Informationen aus dem Krisenstaat zur Lage zu besprechen und das weiterzugeben, Fragen zu klären. Da kommen dann auch ganz viele Fragen aus dem Bereich, wie man dieses oder jenes. Macht, wenn die digitalen Möglichkeiten nicht mehr zur Verfügung stehen. Und in dem Umfeld wurden dann eben auch die Maßnahmen zur Krisenbewältigung besprochen. Und wie geht es weiter? Und wie sehen die zeitlichen Perspektiven aus? Aber gerade in den ersten Tagen war das die Hölle, kann man sagen, denn es gibt ganz viele Anfragen. Auch das Ministerium war vor Ort. Vom CERT-Hessen [Anm. d. Red.: Computer Emergency Response Team] war jemand vor Ort. Das LKA und Staatsanwaltschaft kommt vor Ort und ermittelt und man hat die externen Dienstleiste zu koordinieren. Das war alles am ersten Tag. Hat man da schon ganz viele an Bord. Das hat super funktioniert mit diesem incident-response auch mit externen und die Hilfsbereitschaft von anderen Hochschulen war auch groß. Hat man ganz viele Unterstützungsangebote. Aber es ist natürlich ja, das muss man auch alles bewältigen in der Anfangsphase und ganz viele, ganz viele Entscheidungen treffen. Das hat aber. Gut funktioniert, denn wir hatten dann hier im Hochschulrechenzentrum auch so eine Koordinationsgruppe, also eine Art IT-

Notfallstab, wo wir die Maßnahmen, die hier im Haus dann stattfinden, mussten auch koordiniert haben. Und dann die verschiedenen Teams, die die Schadensanalyse gemacht haben oder auch so Wiederaufbau koordiniert haben. Und die Kommunikation Richtung Uni intern und auch Richtung Öffentlichkeit, die lief komplett über das Präsidium beziehungsweise über die Pressestelle. Das war auch wichtig, dass uns da der Rücken freigehalten wurde, uns um unsere Aufgaben, Schadensanalyse, Schadensbewältigung zu kümmern und dann nicht Interviews mit Presse-Teams oder so was zu führen. Das ist sehr stark abgeschirmt worden und das hat uns sehr weiter geholfen.

[pgg]: Vielleicht dazu noch mal eine Frage. Ich erinnere mich noch, ich hatte den Eindruck, dass die Pressearbeit von Anfang an sehr offen und in so einem guten Sinne auch freimütig war. Die Uni hat nicht versucht, das zu verharmlosen oder abgewimmelt oder so, sondern ist eigentlich sehr freimütig damit umgegangen. War das von Anfang an klar oder wurde da auch diskutiert, ob man sich irgendwie stärker schützt oder dass man sich vielleicht eher in der Kritik sieht oder so?

[Stenke] Das ließ sich ja nicht verheimlichen. Also das war jetzt auch kein Vorfall, den man hätte, irgendwie unter den Teppich kehren können. So nach dem Motto war es nur eine Abteilung oder so betroffen. Die komplette Uni war digital tot. Das macht sofort Schlagzeilen. Das war schon klar, dass man da ganz auch offen an die Öffentlichkeit gehen muss. Also wie gesagt, der erste Social Media Post war am Sonntagabend nach dem nach dem Krisenstab. Ich glaube so um 22.30 Uhr oder so. Und das kam dann auch am nächsten Morgen schon als Meldung im Radio, im hessischen Rundfunk, sodass dann hoffentlich viele Mitarbeitende und Studierende dann schon mal Bescheid wussten, denn das war am Anfang halt schon ein Problem, auf welche Art und Weise kommuniziert man. Und es gab dann auch im Nachgang, in den Tagen und Wochen danach Pressekonferenzen. Es gab Video-Statements vom Präsidenten, vom Herrn Murkherjee. Es gab dann intern auch verschiedene Formate. Es gab dann schon am 10.12., also zwei Tage nach dem Vorfall. Informationsveranstaltung in der Uni-Aula für die Uni-interne Öffentlichkeit, für Universitätsangehörige, die war gut besucht. Es gab noch mal eine Folgeveranstaltung zwei Monate später, im Februar. Es gab dann im Laufe der Zeit auch intern viele Rundmails und Informationen auf der Webseite, in der FAQ, und das ist halt auch wichtig, die Studierenden und die Bediensteten zu informieren über den Stand und wie geht es weiter. Und was sind die nächsten Schritte? Wie war da so die Stimmung? Die Stimmung war meines Erachtens von so einem großen Zusammenhalt geprägt. Ja, wir sind angegriffen worden. Wir müssen jetzt sehen, wie wir damit umgehen. Es gab dann auch viele ermunterte Grußbotschaften. Und also wir haben auch Kehrpakete bekommen, Pakete mit Süßigkeiten und so was. Ja, also was war, sie haben ja eingangs schon gesagt, das ist schon Marathon, den man da zu bewältigen hat. Es gab auch viel Frust, und es standen ja Dinge nicht zur Verfügung, die dringend gebraucht wurden. Aber insgesamt gab es keine Schulzuweisung oder wie konnte das passieren und so. Es war immer zielgerichtet auf die Zukunft weniger, auf die Vergangenheit. Da ging es darum, wir haben jetzt die Situation, wie kommen wir da wieder raus? Was sind die nächsten Schritte? Wie machen wir das am besten? In welcher Reihenfolge? Wie kommunizieren wir das? Und im Nachgang war dann eben die Aufgabe zu überlegen, wie kann man sowas in Zukunft verhindern mit Maßnahmen.

[mg]: Was man noch mal so ein Bild davon bekommt, was das alles an Aufgaben sind, die dann anstehen. Auch wie kleinteilig das ist. Ich habe gelesen, 6.000 Geräte mussten

überprüft werden. Wie macht man das? Wie organisiert man das? Mit wie vielen Leuten sitzt man da dann dran?

[Stenke] ganz vielen Leuten und mit ganz vielen USB-Sticks, die dann mit Virenscanner-Software betankt wurden. Also wir hatten da erhebliche logistische Herausforderungen bei dieser ganzen Bewältigung. Und die Prämisse bei den Schadensanalysen und bei den Schadensbehebungen war auch immer Sicherheit geht vor Schnelligkeit. Also wir hatten jetzt nicht den Druck von oben oder von außen oder sowas jetzt so sofort irgendwas wiederherzustellen, sondern es ging immer darum, das sorgfältig genug zu analysieren. Und möglichst sicher dann auch zu machen. Es hätte auch sein können, dass schon Tage zuvor irgendwas ausgebracht wurde, ohne dass wir das gemerkt haben. Deswegen war die Entscheidung, wir überprüfen alles, was Windows basiert, hier betrieben wird an Endgeräten, an Servern, auch wenn das vielleicht nichts mit der Active Directory Domain zu tun hatte. Aber die wurden alle überprüft. Das heißt, wir hatten dann die Aufgabe, Prüfmittel bereitzustellen in Form von USB-Sticks mit Viren-Scanner-Software. Wir hatten am Anfang auch die Herausforderung, dieser Verschlüsselungstrojaner, der ausgebracht wurde, der wurde von den Viren-Scannern noch gar nicht erkannt. Da musste erst eine Erweiterung gebaut werden für die Viren-Scanner, damit diese spezielle Art dann auch tatsächlich erkannt wird. Und wir haben dann USB-Sticks produziert, 700 glaube ich. Am Ende war es über 1.000, weil wir hatten das in mehreren Wellen auch gemacht, die Überprüfungen. Und diese USB-Sticks wurden in die verschiedenen Bereiche verteilt, also IT-Administratoren vom HLZ waren damit beschäftigt, diese Scans durchzuführen, aber auch dezentrale IT-Administratoren und eine ganze Menge Freiwillige, die da mitgemacht haben, von Bediensteten aus verschiedenen Bereichen der Uni. Und wir hatten auch externe Unterstützung, also Kolleginnen und Kollegen von anderen hessischen Hochschulen. Kamen hier vor Ort und haben uns bei diesen Aktivitäten unterstützt und auch die ein oder andere externe Firma. Denn der Scan von einem Endgerät dauert normalerweise ein paar Stunden und das ist dann halt schon bei mehreren tausend Geräten eine Aktion, die sich über einen längeren Zeitraum hinzieht. Und wir haben das auch so gemacht, dass ein Gerät oder ein Institutsnetz erst dann wieder Kommunikation mit dem restlichen Uni Netz aufnehmen konnte oder auch Kommunikation mit dem Internet, wenn alle Geräte dort auch wirklich geprüft waren. Das heißt, es musste dokumentiert werden, was schon geprüft und gescannt worden ist. Und erst wenn das vollständig war, dann haben wir sozusagen das Go gegeben und den Netzwerkszugang wieder freigeschaltet. Und das war auch so ein Prozess, der hat sich über mehrere Wochen hingezogen. Es hing aber auch immer sehr stark davon ab, wie sich die Fachbereiche und Institute dann daran beteiligt haben, denn die waren eben gefordert, diese Dokumentation dann auch beizubringen, dass diese Scans erfolgt sind. Und das hat dann bis Anfang, ich glaube, bis in den Februar rein hat das dann gedauert, bis das letzte Netz dann auch wieder aktiv war.

[pgg]: Gabs besonders schnelle Fachbereiche oder Abteilungen und besonders überraschte Langsamere.

[Stenke] Das gab es sicher, ich will jetzt aber keine Namen nennen, ich habe es auch nicht parat. Aber man hat dann auch gesehen, es gab dann auch so, das fand ich ganz interessant, es gab so Abhängigkeiten, denn die Netzwerke sind bei uns, die orientieren sich an Gebäuden und in manchen Gebäuden sitzen halt verschiedene Fachbereiche. Die haben dann angefangen, sich gegenseitig zu unterstützen. Oder kam dann auch die Frage, wer ist denn da noch und mit wem haben wir denn da Abhängigkeiten? Was sah

es gemeinsam in einem Boden, erst wenn alle … Ihren Job gemacht haben, dann ging es für alle auch weiter. Das hat gut funktioniert.

[mg]: Gab ja sicher auch die Notwendigkeit für pragmatische, sag ich mal, analoge Lösungen auch, um den Betrieb aufrechtzuerhalten. Ein Beispiel, von dem ich gelesen habe, war die Bibliothek, die wieder zurückgegangen ist zu vordigitalen Ausleihmethoden. Ist das ein Stück weit auch was, was Teil solcher Notfallstrategien ist, dass man die analogen Techniken bewahrt, also so einen alten Ausleihzettel noch benutzen zu können und so?

[Stenke] Da gab es verschiedene kreative Lösungen, also dass dieses mit den Auslasszetteln der OB, das ist sicherlich eins davon, das ist aber nicht in allen Fällen möglich. Ja, also bei diesem Prozess ging das, da konnte man halt auf die alten Zettel, die noch, ich glaube auch sogar noch irgendwo auf Lager waren, zurückgreifen. Aber im Nachgang gab es dann halt auch das Problem, das dann wieder mit dem digitalen Auslasssystem zu synchronisieren. Aber das ist Bestandteil von so einem Notfall. Management oder Notfallvorsorgeplanung, dass man sich überlegt, wie kritisch sind die Systeme, die man betreibt und die Anwendungen, wie lange darf das maximal ausfallen, was toleriere ich für einen Datenverlust und was gibt es für Umgehungslösungen in dem Umfeld. Da wurden bei dem Vorfall 2019 halt, ja, da war dann Kreativität gefragt. Also die Anfangskommunikation, die lief dann sicherlich sehr viel über Messenger-Dienste. Es sind private E-Mail-Adressen dann teilweise verwendet worden in den ersten Tagen, bis wir dann kurz vor Weihnachten 2019 das Uni-E-Mail-System wieder so weit hatten, dass das genutzt werden konnte oder mit LTE-Access Points und für bestimmte Geräte dann doch einen Internet-Zukauf haben zu können. Also solche Sachen sind auch rausgerollt worden. Da gab es halt viele Workarounds. Aber es ist natürlich gut. Wenn man sich im Vorfeld im Rahmen von der Notfallvorsorgeplanung Gedanken macht, wie man das realisieren kann im Falle eines Falles. Wenn trotz aller Vorsichtsmaßnahmen, Sicherheitsmaßnahmen die digitalen Systeme nicht zur Verfügung stehen. Aber es geht sicherlich nur in einzelnen Ausnahmefällen.

[pgg]: Haben Sie im Nachhinein dann auch neben besseren Vorsorgeplänen tatsächlich was verändert, umgebaut, weil Sie anlässlich des Vorfalls gemerkt haben, so sollten wir nicht aufgestellt sein?

[Stenke] Also wir haben die Krise als Chance genutzt und beim Wiederaufbau dieser Windows-basierten Infrastruktur das nicht eins zu eins gemacht, so wie das vorher war. Das war eine Infrastruktur, die Anfang der 2000er aufgebaut worden ist, natürlich immer wieder aktualisiert und so weiter. Aber das entwickelt sich ja auch weiter, wie man da konzeptionell vorgeht und wir haben beim Wiederaufbau. Das einmal komplett neu gemacht. Wir hatten externe Unterstützung und haben dann diese komplette Windows-Domain-Struktur nach den aktuellen Erkenntnissen, wie man das möglichst sicher aufbauen und betreiben kann, dann auch neu aufgebaut und konnten uns dankenswerterweise dann auch die Zeit dafür nehmen, das zu planen und umzusetzen. Da hat uns das Präsidium den Rücken freigehalten, denn das war jetzt auch ein ganz wichtiger Baustein. Bessere Grundlage zu schaffen, dass das in Zukunft in der Form nicht mehr auftritt. Und das sind halt schon massive strukturelle Veränderungen, die man da machen muss. Und solche Dinge, das machen sie nicht mal ebenso im Lauf im Betrieb. Das ist schon ein größerer Aufwand. Aber wir konnten die Krise, die wir hatten, als Chance nutzen, diese Veränderung umzusetzen. Wir haben auch in anderen Bereichen deutlich Veränderungen gemacht. Wir haben eine IT-Sicherheitsstrategie

entwickelt 2020. Und die jetzt in den letzten Jahren auch umgesetzt. Dazu gehört zum Beispiel ein Aufbau einer geeigneten Organisation für IT-Sicherheit. Wir haben jetzt seit einem guten Jahr einen eigenen hauptamtlichen Informationssicherheitsbeauftragten. Wir haben seit mehreren Jahren jetzt drei Kollegen, die sich um operative IT-Sicherheitsthemen kümmern, wie aufspüren von sicherheitsrelevanten Vorgängen und dem Nachgehen. Das ganze Thema ist personell besser aufgestellt. Der Informationssicherheitsbeauftragte wird von einem ISMS-Manager unterstützt, also jemanden, der sich um so die Informationssicherheitsmanagement-Systemprozesse kümmert. Wir machen ein Informationssicherheitsmanagement nach BSI IT-Grundschutz, das wir aufgebaut haben. Und wir haben neben diesem deutlich verbesserten Aufbau der Windows-Domain-Infrastruktur. Auch in anderen Bereichen technisch aufgerüstet. Also beispielsweise E-Mail-Security verbessert, Schadsoftware-Filter, weil das ist, so ein Haupteinfallstor für Fishing-Angriffe oder auch für Schadsoftware, um da das Risiko zu vermindern. Wir haben im Bereich Netzwerksicherheit diverse Maßnahmen getroffen. Wir haben aber auch im Bereich der Nutzenden Awareness-Maßnahmen, Schulungsmaßnahmen, Fishing-Simulationen, die wir durchführen. Das ist ein wichtiger Punkt. Also bei der Sicherheit gibt es jetzt nicht einen Hebel, wo man drehen kann, sagen kann, okay, ich führ jetzt mal dieses oder jenes ein, dann ist gut. Sondern das ist ein ganzes Bündel an Maßnahmen und Prozessen, die man eben braucht. Und ein Bestandteil ist halt auch ein strukturiertes Notfallmanagement nach BSI. Da gibt es auch entsprechende Vorgaben, wie man das machen sollte. Das haben wir auch eingeführt und machen da auch Übungen für solche möglichen Angriffe und Vorkommnisse.

[mg]: Ich würde gerne mal bei der aktuellen Angriffslage bleiben. Man liest manchmal so irre Zahlen, mehrere Millionen registrierte Angriffsversuche pro Quartal. Also wie muss man sich das vorstellen? Hat die Universität so eine Art Firewall, wo die ganze Zeit irgendwelche trivialen Angriffe, die man schon gar nicht mehr registriert, dran abprallen und dann ab und zu passiert mal was Interessantes oder was Gefährliches?

[Stenke] Ja, also wir haben natürlich eine Firewall und an der prallt der Allermeiste ab. Und so kommen dann halt solche Zahlen zusammen. Wenn dann jemand versucht, auf irgendwas zuzugreifen, die Firewall, lässt das aber nicht zu, dann ist das ein potenzieller Angriff. Ob der dann erfolgreich gewesen wäre, wenn es durchgekommen wäre durch die Firewall oder nicht, das sei mal dahingestellt. Aber es wird natürlich ständig probiert. Also wenn Sie jetzt einen Server einfach ins Internet stellen. Dann dauert es nicht lange und dann wird dann halt probiert, sich über Kommandozeile, über SSH oder was auch immer da anzumelden mit Standardpasswörter, mit Standard Benutzer Accounts. Ja, es wird versucht, Sicherheitslücken, die in Software bestehen, auszunutzen. Die Gefahr ist nach wie vor da und das passiert ja auch ständig und gefühlt immer öfter. Man muss da halt ständig am Ball bleiben und schauen, ist man von was betroffen? Wie ist das Risiko? Wie bewertet man das? Sind alle Systeme aktuell? Das sind die täglichen Herausforderungen.

[mg]: Sie sagten ja gerade schon auch, E-Mails sind eigentlich heikel. Da ist man schuld, man braucht Awareness. Und dann gibt es sicherlich auch verbindliche Richtlinien im Bereich IT-Sicherheit, die für alle Hochschulmitglieder gelten. 25.000 Studierende, 5.500 Mitarbeitende. Ist das das Ziel, dass das auf der individuellen Ebene von allen gewusst und umgesetzt wird?

[Stenke] Das ist schon das Ziel. Wir bieten E-Learnings an in dem Umfeld, was im Wesentlichen von den Bediensteten genutzt wird. Als Informationsquelle, wir machen aber hauptsächlich auch solche Phishing-Simulations-Kampagnen. Das hat den Vorteil, dem kann sich niemand entziehen. Solche Simulations-Mail bekommt halt jeder im Abstand von circa einem Monat mal so ins Postfach zu verschiedenen Themen. Das ist auch eine gute Trainingsmaßnahme und wird auch ganz gut akzeptiert von den von den Nutzenden. Das heißt, Sie schicken selbst was raus und gucken, wer fällt drauf rein? Ja, das ist so, wer fällt drauf rein. Das ist immer die Frage, wem man das so formulieren. Da ist niemand gegen gefeit. Also es muss nur. Ich sage immer, es muss nur in den Kontext passen. Ich warte auf irgendwas. Und das passt gerade in meine Erwartung. Und dann klickt man halt vielleicht doch drauf. Ja, kann mir auch passieren, obwohl ich jeden Tag auch solche Sachen zur Prüfung bekomme und man oft auf den ersten Blick sieht, ist das, was Recht ist, oder ist das, was Unrecht ist. Man muss nur im Zeitdruck und so. Das kann jedem passieren. Das Feedback der Benutzer war, als wir das eingeführt haben, vor ungefähr drei Jahren, überraschend positiv. Also ich habe damit deutlich mehr Gegenwind gerechnet, muss ich sagen, weil es ja schon so eine Komponente hat. Okay, ihr führt mich hier aus Glatteis. Aber ich denke, bei uns hat das auch damit zu tun, dass viele den Vorfall miterlebt haben und das auch noch mal eine andere Awareness oder Bereitschaft geschaffen hat, solche Maßnahmen zu akzeptieren oder einzusehen. Ja, das ist schon… Das ist schon wichtig und jeder muss so oder sollte seinen Beitrag leisten. Es sind eigentlich alle gefordert. Man kann nicht sagen, okay, ihr HRZ oder ihr operative IT-Sicherheit, du Informationssicherheitsbeauftragte sorgt noch für Sicherheit. Und ich muss da nichts machen. So ist es nicht. Es müssen alle mitziehen. Es müssen auch die Nutzen in dem Prozess mitgenommen werden. Und das funktioniert meines Erachtens ganz gut bei uns, was sicherlich auch mit der Erinnerung an 2019 zu tun hat. Da ist die Bereitschaft sicherlich größer.

[mg]: Gibt es auch Software oder Nutzungsweisen von Software, die Sie verbannt haben, sage ich jetzt mal, von der Hochschule oder wo man sagt, das möchte man aus Sicherheitsgründen nicht mehr einsetzen?

[Stenke] In Bezug auf früher? Ja, wenig. Also man hat halt in diesem Bereich Forschung und Lehre. Braucht man halt gewisse Freiheiten, dass die Forscher auch mal Sachen auszuprobieren. Wir warnen aber durchaus vor ja dann auch mal vor kritischen Sachen. Also Auslandsreisen beispielsweise. Wenn jemand nach China fährt und soll sich dann das WeChat installieren als App, dann empfehlen wir beispielsweise das dann auf einen separaten … Smartphone nur für den Zweck zu machen. Aber wir haben jetzt keine harten Vorgaben, dass bestimmte Sachen nicht genutzt werden dürfen. In der Verwaltung gibt es ein bestimmtes Set an Software, das im Einsatz ist. Das wird auch noch abgestimmt. Aber so im Bereich Forschung und Lehre jetzt weniger.

[pgg]: Jetzt muss man sicher auch über Kosten reden. Also für die Uni war das nicht nur ein Schlag, was Abläufe angeht, sondern sicher auch teuer. Sie haben auch beschrieben, es ist dann nachträglich umgebaut worden, eine andere Struktur eingeführt worden. Es gibt Personal mit neuen Rollen und so weiter. Kann man abschätzen, was das für einen Umfang an Schaden verursacht hat?

[Stenke] Also der direkte Schaden oder der finanzielle Schaden, den wir hatten, im Sinne von externer Unterstützung, die gebraucht wurde, vielleicht auch Hardware für den Neuaufbau von bestimmten Dingen, Arbeitszeit von Mitarbeitenden, das belief sich auf 1,7 Millionen Euro. Das sind die Kosten, die dann direkt angefallen sind, da ist es aber jetzt

kein Arbeitszeitausfall von Forschern, die IT nicht nutzen konnten, das ist da nicht mit eingerechnet. Das sind so die direkten zuordenbaren Kosten bis Mitte Ende 2020 ungefähr, also bis zum Abschluss der Schadbehebungs- und Wiederaufbaumaßnahmen.

[pgg]: Da auch finanzielle Unterstützung für die Uni erfolgt. Also hat man gesagt, sie kriegen Landesmittel zusätzlich oder gab es eine Versicherung.

[Stenke] Ne, eine Versicherung gibt es nicht. Und dafür gab es jetzt auch für den Ausgleich dieses Schadens gab es meines Wissens keinen direkten Landesmittel. Aber es gibt ja immer so Projektförderung vom Land. Im Digitalpakt beispielsweise, der 2020 aufgelegt worden ist, da gab es dann ein neues Projekt Steigerung IT-Sicherheit von den Hochschulen gefordert oder auch gewünscht und vom Land mit finanziellen Mitteln unterstützt. Und da haben wir erhebliche Förderung bekommen in den letzten Jahren, die den Betrag, den ich genannt habe, sicherlich übersteigt. Ja, daraus haben wir Sachmittel finanziert. Daraus haben wir jetzt auch als Anschub die Personalstellen finanziert im IT-Sicherheitsbereich, die jetzt neu geschaffen worden sind. Das ist in dem Bereich auf jeden Fall eine super Anschubfinanzierung. Muss die Uni jetzt aber in den Folgejahren selbst stemmen, ist aus meiner Sicht aber… absolut erforderlich. Ja, die Bedrohungslage nimmt nicht ab, die nimmt eher zu und man muss da einfach mehr machen, als man es vielleicht vor zehn Jahren gemacht hat. Das glaube ich mittlerweile ist allen vor Augen geführt worden. Es gab auch weitere Angriffe auf Hochschulen in den letzten Jahren. Das reißt nicht ab.

[pgg]: Hat der Fall Gießen auch den anderen Hochschulen geholfen, sich einzustellen, umzustellen? Sind sie auch von anderen Hochschulen, vielleicht auch aus anderen Bundesländern, kontaktiert worden, die dann von ihnen in Echtzeit lernen wollten?

[Stenke] Ja, also wir hatten natürlich kurz nach dem Vorfall dann auch viele Anfragen dazu. Wir haben das aber kanalisiert gemacht. Also wir haben zum einen den Artikel in der ABI-Technik veröffentlicht zu dem Vorfall. Und ich habe bei einigen Konferenzen teilgenommen, ab Herbst 2020 ungefähr. Ich habe da halt auch ausführlich berichtet, was passiert ist und auch berichtet über unsere Maßnahmen. Die wir dann danach getroffen haben. Also Interesse war schon sehr groß. Vor allen Dingen auch von den anderen hessischen Hochschulen, weil die natürlich näher an uns dran saßen und uns auch unterstützt haben und das mit eigenem Personal die Schadensbewältigung dann auch teils live erlebt haben. Da gab es schon intensiven Austausch. Und insgesamt hat es sicherlich auch anderen geholfen, anderen Rechenzentren, anderen IT-Verantwortlichen bei den Hochschulen das Thema IT-Sicherheit höher priorisiert zu bekommen bei ihren Präsidien und auch Wie gesagt, im Land hat, das dann auch einen ganz anderen Stellenwert bekommen dadurch, dass es im Digitalpakt dann als eigenes Projekt hochschulübergreifend gefördert worden ist. Also es hat sicherlich geholfen als in Anführungszeichen Awareness-Maßnahme, dass man da mehr tun muss und dass das massive Auswirkungen haben kann, wenn so ein Angriff erfolgreich ist.

[mg]: Sie sagten ja, man tauscht sich aus zu dem Thema, es gibt Konferenzen, es gibt einen Erfahrungsaustausch. Aber gibt es darüber hinaus auch, sag ich mal, eine Institutionalisierung dieser Solidarität? Oder ist am Ende dann doch jede Hochschule für sich zuständig, die anderen können unterstützen, aber man schafft letztlich, sag ich mal, wirklich eine feste Institution eines Netzwerks, dass man dann gemeinsam vielleicht auch Methoden entwickelt und das als gemeinsame Aufgabe.

[Stenke] Also im Rahmen des Digitalparks-Projekts gibt es sowas tatsächlich, aber dann eher so auf Basis von einzelnen Maßnahmen. Da haben wir einen intensiven Austausch. Den werden wir jetzt auch, so ist es zumindest geplant, über das Projekt Ende hinaus aufrechterhalten, dass man sich zu solchen Themen austauscht und abstimmt und auch mit dem Ziel, dann Dinge gemeinsam zu machen. Das gibt es hier in Hessen oder den Universitäten. Das Thema Together First, dass nicht jeder alles für sich allein macht, sondern dass man sich auch zusammentut mit der Bereitstellung von bestimmten Diensten. Das gibt es beispielsweise in Form von der Hessenbox, die jetzt in Kassel auf ein neues System umgestellt worden ist und hessenweit bereitgestellt wird. Das ist aber auch denkbar im Bereich IT-Sicherheit, dass man bestimmte Dinge wie sowas wie ein Security Operations Center, was die IT-sicherheitsrelevanten Ereignisse in der Infrastruktur. Analysiert und beobachtet, dass man das hochschulübergreifend macht, entweder was aufbaut oder gemeinsam einkauft. Solche Aktivitäten gibt es schon. Im Moment haben wir das in der Form noch nicht, aber wird sicherlich in Zukunft kommen, weil es absolut Sinn macht, sich da auch zusammen zu tun, um das Ganze dann effizienter und günstiger für alle Beteiligten zu machen. Aber die Hochschulen sind halt unterschiedlich weit. Ja, das ist dann halt auch eine gewisse Herausforderung. Oder haben auch unterschiedliche Schwerpunkte und Prioritäten. Beispielsweise haben wir jetzt vor ein paar Jahren unsere Windows-basierte Infrastruktur neu aufgestellt. Haben da jetzt erstmal keinen Bedarf an größeren Weiterentwicklungen. Das sieht bei anderen Hochschulen vielleicht anders aus.

[pgg]: Ich habe noch mal eine Frage zu der Kommunikationslage, so in der akuten Phase. Hatten Sie da auch mit Falschmeldungen, mit Gerüchten und mit solchen Dingen zu kämpfen? Oder ist die sachliche Lagebeschreibung einfach gut durchgedrungen? Und insofern ging es nur um Information.

[Stenke] Also in erster Hand war ich da nicht so dicht dran, also aber über Social Media gab es dann schon so den einen oder anderen Kommentar, mit dem die Kolleginnen von der Pressestelle umgehen mussten. Also da gab es ab und zu mal was, wo irgendwas in Richtung Falschmeldungen oder irgendwelche unrealistischen Forderungen kam, dem man dann begegnen musste. Und da war eigentlich immer das Thema dann schnell zu reagieren, bevor sich irgendwas verbreitet. Da kann ich mich noch dran erinnern. Dann auch mal Fragen kamen, hier, da ist die Meldung, wie ist denn das wirklich? Und dass wir dann von IT-Seite eine Rückmeldung gegeben haben und dann dem begegnet wurde, das war jetzt nach meiner Erinnerung kein so Riesenthema. Wie gesagt, der Zusammenhalt war schon recht gut insgesamt bei der Krise.

[mg]: Ist das auch ein Learning, vielleicht zu viel gesagt, aber eine gewisse Erleichterung, die Erfahrung zu machen, dass dann doch das Kollegium und alle Hochschulmitarbeiter so gut mitarbeiten, sag ich mal, die Krise zu bewältigen, ist das ein Stück weit auch eine Ressource? Oder was, worauf man sich nicht verlassen darf bei der Planung?

[Stenke] Das hängt wahrscheinlich von der Situation ab, aber es war natürlich schon extrem, hilfreich, dass man da nicht noch massiven Gegenwind- und Rechtfertigungsdruck und was auch immer hatte. Und wichtig war da auch aus meiner Sicht so die klare Kommunikation. Wie ist der Stand? Wie geht es weiter? Und wann steht was wieder zur Verfügung? Und diese Prognosen dann so zu machen, dass man sie auch realistisch einhalten kann. Das hat gut funktioniert. Und das ist jetzt meine persönliche Einschätzung. Man ist erstmal in ein tiefes Loch gefallen. Digital, dass man

dann eine Perspektive hat, wie geht das weiter und was sind die Schritte und wie ist die Perspektive. Das ist aus meiner Sicht dann wichtig und das haben wir immer versucht zu geben. Das hat sich aber Monate hingezogen, dieser Wiederaufbau. Viele sagen, ging schnell wieder, also alles das, was so Linux-basiert, E-Learning-System, das lief Anfang Januar wieder. Wir haben auch vom Timing her eigentlich Glück gehabt, kann man sagen, das war vor der Pandemie. Wir waren noch nicht komplett abhängig von den ganzen digitalen Werkzeugen. Das kam dann im März während des Wiederaufbaus. Das war auch noch mal so eine Herausforderung. Aber es war vor der Pandemie und es war kurz vor der Weihnachtspause, wo dann kein Lehrbetrieb war. Und als der Lehrbetrieb wieder startete Anfang Januar, waren die für die leere relevanten Systeme wieder da. Das war auch gut und das ging dann halt schrittweise vorwärts, auch wenn es dann bis in den Herbst hineingedauert hat, bis die letzte Fachanwendung, wie irgendwelche Lizenzserver oder irgendwas Spezielles in der Verwaltung dann wieder aufgebaut war. Das war dann hinten raus schon eine lange Strecke, aber am Anfang waren die die Fortschritte halt deutlich dichter. Und das war, glaube ich, auch wichtig, um den Nutzen eine Perspektive zu geben und die sozusagen dann auch. Ja, mit bei der Stange zu halten, dass es vorwärts geht und dass die Ungewissheit nicht so groß ist.

[mg]: Letzter Punkt, noch mit Blick nach vorne, diese permanente Angriffswelle, mit der sich die Rechenzentren jeden Tag konfrontieren müssen oder die sie irgendwie organisieren müssen, mit der sie irgendwie umgehen müssen. Ist das was, womit man sich jetzt einfach abfindet und arrangiert oder ist das Ziel schon, oder gibt es auch Bestrebungen, diesen Zustand irgendwie zu beenden oder auch diesen direkten Druck von den Rechenzentren runterzunehmen und da irgendwas platt zwischendurch?

[Stenke] Also ich sehe nicht, dass sich das substanziell ändert, denn es gibt immer mehr Systeme, es gibt mehr Software, die naturgemäß dann ihre Schwachstellen hat. Da wird immer was gefunden und also immer die Motivation für die Angreifer sind ja Verschiedene. Ja, da ist sicherlich viel kriminelle finanzielle Interessen dahinter. Aber es gibt ja auch andere, wie staatliche Akteure, Wirtschaftsspionage, politisch motivierte. Angriffe auf kritische Infrastruktur, gut, das sind wir jetzt nicht, ja, das betrifft uns jetzt weniger. Aber ich sehe nicht, dass das weniger wird. Das ist das alte, das ist so ein Katz-und-Maus-Spiel. Also Beispiel heute, es gab eine Meldung über kritische Sicherheitslücken in Druckersoftware, Drucker-Firmware. Dadurch kann Drucker ganz einfach von einem Angreifer übernommen werden und er kann die Administration des Druckers übernehmen oder mehr. Das ist beispielsweise ein Fall, mit dem wir jetzt gerade umgehen. Und dagegen Maßnahmen treffen, um zu verhindern, dass das tatsächlich ausgenutzt werden kann. Da kommen ständig neue Dinge und ich sehe jetzt persönlich nicht, dass sich das in absehbarer Zeit ändert.

[mg]: Trauriges Schlusswort.

[pgg]: Trauriges Schlusswort.

[Stenke] Ja, aber jeden Tag eine neue Herausforderung, im Zweifelsfall. Also es macht das Gebiet aber auch spannend, es ist nicht langweilig. Man hat immer seine Herausforderung und interessante Themen, mit denen man sich beschäftigt.

[mg]: Und damit ist dieses Digitalgespräch zu Ende und wir bedanken uns bei Matthias Stenke von der Justus-Liebig-Universität Gießen für diese spannenden Einblicke und das interessante Gespräch. Viele Grüße und wie immer auch vielen Dank an Sie, liebe

Zuhörerinnen und Zuhörer, für das Interesse und die Aufmerksamkeit. Wenn Sie mögen, hören wir uns in drei Wochen wieder zur nächsten Folge des Digitalgesprächs, einem Podcast von CWDI, dem Zentrum für verantwortungsbewusste Digitalisierung.

This work is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/