# Krise als Chance

KONRAD ADENAUER STIFTUNG

**Politisches Bildungsforum Rheinland-Pfalz**

# » Die Krise bietet die Chance, Cybersicherheit in den Fokus zu rücken.«

***Jonas Grasediek***

*Experte für Cybersicherheit, Mitarbeiter in einem Computer Emergency Response Team*

**Konrad-Adenauer-Stiftung:**
Herr Grasediek, in unserem Webinar „Sichere Kommunikation in Zeiten von COVID-19" haben Sie auf verschiedene Handlungsmuster hingewiesen, um sich online zu schützen. Sehen Sie eine gesteigerte Notwendigkeit dafür in der sogenannten Corona-Krise?

**Jonas Grasediek:**
COVID-19 hat neben Unternehmern auch viele Bürger sehr verunsichert, da die meisten von uns bisher mit keiner vergleichbaren Situation konfrontiert waren. Sowohl auf Seiten der Arbeitgeber als auch der Arbeitnehmer mussten sich Menschen plötzlich damit auseinandersetzen, dass ein Großteil der Arbeit im Home-Office absolviert werden muss. Dies hatte zur Folge, dass viele Unternehmen in möglichst kurzer Zeit erst einmal eine geeignete Infrastruktur für die Arbeit von zu Hause errichten mussten. Parallel dazu mussten sich viele Arbeitnehmer mit einer für sie gänzlich neuen Arbeitsweise auseinandersetzen, da nicht nur die Einwahl bzw. die Verbindung über das Internet zum Unternehmen erforderlich war, sondern nun auch die eigene Infrastruktur zu Hause wesentlicher Teil der täglichen Arbeit wurde.
In einem Unternehmen habe ich in der Regel eine eigene IT-Abteilung oder einen IT-Dienstleister, die sich täglich mit Themen wie Infrastruktur, elektronischer Kommunikation und im besten Fall ausführlich mit Cybersicherheit beschäftigen. Da sprechen wir dann von Profis, die eine Ausbildung und u. U. ein Studium absolviert haben und somit über eine Menge Fachwissen und Erfahrung verfügen. Das bedeutet, im Unternehmen habe ich neben einer gesicherten Infrastruktur (z. B. Firewall, getrennte Netze, Offline-Backups, etc.) Fachleute auf die ich zurückgreifen kann.
Zu Hause ist das hingegen eine völlig andere Situation. Da steht in der Regel ein Router und ein PC, der im besten Falle regelmäßig Updates erhält und auf dem ein Antivirenprogramm läuft. Aber ich kann von keinem meiner Nicht-IT-Mitarbeiter erwarten, dass dort eine Infrastruktur mit den Sicherheitsmaßnahmen des Unternehmens steht und dass dieser sich tiefgehend mit derartigen Themen beschäftigt. Das wäre für die jeweilige Person nicht

nur finanziell, sondern auch zeitlich kaum zu bewältigen.
Aber genau diesen Mangel an speziellem Wissen in Kombination mit der aktuell herrschenden Unsicherheit machen sich die Angreifer zunutze. So werden beispielsweise gefälschte Webseiten mit vermeintlichen Informationen zu COVID-19 oder Webshops auf denen man besonders günstig Masken, Desinfektionsmittel oder dergleichen erwerben kann, im Internet bereitgestellt und ahnungslose Benutzer zum Aufruf dieser Seiten verleitet. Oftmals enthalten diese Seiten einen Schadcode, der sich auf dem Rechner des Benutzers einnistet und dort erheblichen Schaden verursachen kann. Dies stellt dann auch ein erhebliches Risiko für die Unternehmen dar. Wählt ein Benutzer sich mit einem infizierten Rechner in das Unternehmen ein, kann sich der Schadcode u. U. auch im Firmennetz einnisten und dort weiteren massiven Schaden anrichten.
Grundsätzlich bestand dieses Risiko schon vor COVID-19 und ist keine neue Gefährdung, aber die aktuelle Situation und die vergangenen drei Monate haben gezeigt, dass die Verunsicherung vieler Menschen es den Kriminellen leichter gemacht hat Angriffe auszuführen.
Daher besteht aus meiner Sicht eine gesteigerte Notwendigkeit, sich in Zeiten von COVID-19 online zu schützen.

**Konrad-Adenauer-Stiftung:**
Wie schätzen Sie den Aufklärungsbedarf des Durchschnittsnutzers ein? Muss mehr getan werden?

**Jonas Grasediek:**
Bei Betrachtung des Durchschnittsnutzers ist aus meiner Sicht auf jeden Fall noch Aufklärungsbedarf vorhanden. Das liegt aber nicht daran, dass der Durchschnittsnutzer sich ggfs. nicht ausreichend informiert oder sich nicht mit der Thematik beschäftigen möchte. Mein Eindruck ist vielmehr, dass die Fülle an Informationen die sich insbesondere im Internet finden lässt, einen Durchschnittsnutzer schlicht und ergreifend überfrachten kann. Tippt man bei einer Suchmaschine im Internet „Maßnahmen gegen Cyberkriminalität" ein, erhält man rund 399.000 Ergebnisse. Da ist dann alles Mögliche dabei wie z. B. Sicherheitshinweise bekannter Antivirus- und Firewallhersteller, Nachrichtenseiten aus aller Welt sowie die Webseiten staatlicher Institutionen wie etwa das BMI. Für den Durchschnittsnutzer besteht jetzt die Herausforderung herauszufiltern, welche Informationen für ihn relevant und hilfreich sind.
Aus meiner Sicht muss der Durchschnittsnutzer hier bessere Unterstützung erhalten, um optimal über die Gefahren im Internet aufgeklärt zu werden. Im besten Falle sollten bereits Schüler grundlegende Verhaltensweisen zum Schutz im Internet erlernen, sodass sie bereits in jungen Jahren wissen wie sie Risiken und konkrete Gefahren erkennen und möglichst vermeiden können. Für erwachsene Nutzer würde ich auf jeden Fall die Teilnahme an Webinaren wie dem der Konrad-Adenauer-Stiftung empfehlen, da hier wesentliche Informationen möglichst kompakt vermittelt werden, um zumindest eine grundlegende Sensibilisierung zu erreichen.
Einen Tipp, den ich auch in der Präsentation zum Webinar gegeben habe, ist das BSI für Bürger. Es handelt sich hierbei um eine Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welche sich in erster Linie an Durchschnittsnutzer ohne tiefgehende IT-Kenntnisse richtet. Neben Informationen über grundlegende Begrifflichkeiten im Kontext der Cybersicherheit kann man sich hier auch über aktuelle Geschehnisse und Risiken durch Cyberkriminalität informieren. Des Weiteren besteht die Möglichkeit einen Newsletter zu abonnieren, um regelmäßig Hinweise zu aktuellen Viren und Patches zu erhalten.

**Konrad-Adenauer-Stiftung:**
Hat sich Ihre Arbeit im Bereich der Cybersicherheit seit Beginn der Krise verändert?

**Jonas Grasediek:**
Zurzeit erhalte ich nahezu täglich Informationen zu neuen Angriffen, Betrugsversuchen und ähnlichen Ereignissen, die von Angreifern unter dem Deckmantel COVID-19 durchgeführt werden. Hierzu zählen insbesondere gefälschte E-Mails mit vermeintlichen Soforthilfe-Benachrichtigungen, maliziöse Webseiten, die angeblich Informationen zu COVID-19 bereitstellen sowie gefälschte bzw. betrügerische Internetshops, auf denen ahnungslose Menschen um ihr Geld gebracht werden.
Ein wesentlicher Teil meiner Arbeit im Bereich der Cybersicherheit ist es nun, solche Gefährdungen frühestmöglich wahrzunehmen, zu prüfen ob und wie diese unsere Zielgruppen gefährden und schließlich mit den mir zur Verfügung stehenden Mitteln entgegenzuwirken. Ein weiterer Teil ist das

Informieren sowie die Sensibilisierung der Zielgruppen auf Basis der gewonnenen Informationen. Das bedeutet, ich informiere die Zielgruppen über aktuelle Angriffsszenarien und Gefährdungen, wie z. B. die o. g. betrügerischen Webshops, und gebe je nach Möglichkeit eine entsprechende Handlungsempfehlung zur Vorbeugung mit.
Im Prinzip hat sich diese Vorgehensweise in Zeiten COVID-19 nicht verändert, da wir auch vorher schon mit den o.g. Angriffsszenarien konfrontiert waren. Was sich allerdings verändert hat, ist die von den Angreifern missbrauchte Thematik. Daher ist auch in Zukunft mit Cyberkriminalität zu rechnen, die der jeweils aktuellen Situation angepasst ist.

**Konrad-Adenauer-Stiftung:**
Rechnen Sie mit einem erhöhten Aufkommen von Cyberkriminalität durch die Verlagerung krimineller Aktivitäten ins Netz?

**Jonas Grasediek:**
Ja, damit rechne ich fest und das ist auch ein Trend, den man seit Jahren beobachten kann. Immer mehr Firmen verlagern ihr Geschäftsmodell ins Internet und bieten dort hauptsächlich ihre Dienstleistungen an. Das gleiche haben auch die Kriminellen gemacht und ihre Geschäftsmodelle ebenfalls ins Internet verlagert. Das Internet bietet aus Sicht der Kriminellen gleich mehrere Vorteile. Zum einen machen sie sich die Unwissenheit bzw. die fehlende Expertise vieler Benutzer zunutze und können dadurch verhältnismäßig einfach Geld durch Aktivitäten wie Phishing, Erpressung und gefälschte Webshops erbeuten. Zum anderen spielt den Kriminellen die Möglichkeit zur relativ einfachen Verfälschung der eigenen Identität in die Hände. Ein Angreifer kann sich beispielsweise als ein Bekannter seines Opfers ausgeben und dieses dazu verleiten auf Links zu klicken, die es zu maliziösen Webseiten oder gefälschten Onlineshops führen.
Da auch in Zukunft immer mehr Geschäfte im Internet stattfinden, ist aus meiner Sicht auch mit einer Zunahme der Cyberkriminalität zur rechnen.

**Konrad-Adenauer-Stiftung:**
Wo sehen Sie die größte Gefahr für Nutzer während der Krise?

**Jonas Grasediek:**
Aktuell sehe ich die größte Gefahr für die Nutzer darin, dass ihre Verunsicherung von den Angreifern gezielt ausgenutzt wird und dies zu erheblichen Schäden bei den Opfern führt, sei es finanzieller oder persönlicher Art. Dies zeigen auch die aktuell im Internet stattfindenden kriminellen Aktivitäten, wie z. B. die gefälschten COVID-19 Informationsseiten auf denen Schadcode verteilt wird oder Phishingmails von der vermeintlichen Hausbank, die angeblich zur Absicherung der Finanzen die Zugangsdaten ihrer Kunden benötigt. Nutzer, die solche Webseiten aufrufen oder ihre Zugangsdaten im Rahmen von Phishing preisgeben, müssen nicht nur mit Risiken wie Datenverlust und Virenbefall, sondern auch mit finanziellen Schäden in nicht unerheblicher Höhe rechnen.
Aber auch für Unternehmer und Selbstständige besteht eine große Gefahr. Und zwar wurden relativ kurz nach Bekanntwerden der finanziellen Unterstützung durch den Staat, gefälschte E-Mails mit vermeintlichen Anträgen und Links zu vermeintlichen Antragsportalen versendet. Entweder war es dann so, dass der angebliche Antrag im Anhang eine maliziöse Datei war, die den Rechner infiziert und u. a. die Dateien auf dem Computer verschlüsselt hat oder der Link zum angeblichen Antragsportal hat zu einer maliziösen Webseite geführt, die ebenfalls den Rechner infizierte. In anderen Fällen wurden solche Mails auch gezielt für Phishing genutzt indem beispielsweise die Daten des Unternehmers bzw. dessen Firma gezielt abgefragt und im späteren Verlauf für weitere Angriffe genutzt wurden. Beispielsweise könnte ein Angreifer sich mit umfangreichen Daten seines Opfers als jenes Unternehmen bei anderen Geschäftspartnern ausgeben, um weitere Daten zu sammeln oder gezielte Angriffe durchzuführen.

**Konrad-Adenauer-Stiftung:**
Gibt es grundlegende Verhaltensmuster im Umgang mit dem Internet, die Sie jedem Nutzer empfehlen würden?

**Jonas Grasediek:**
Ja, es gibt ein paar Verhaltensmuster, die relativ simpel klingen und auch einfach umgesetzt werden können. In der Vergangenheit hat sich zudem gezeigt, dass ein Großteil von Cyberangriffen bereits durch einfache Maßnahmen teilweise oder sogar ganz hätte vermieden werden können.
Als eine der ersten Maßnahmen würde ich empfehlen die Software stets aktuell zu halten. Eine Vielzahl erfolgreicher Cyberangriffe ist auf Schwachstellen zurückzuführen, die in veralteter Software enthalten

waren und durch ein zeitnahes Update der jeweiligen Software beseitigt worden wären.
Als weitere Maßnahme empfehle ich stets regelmäßig Offline-Backups anzulegen. Das bedeutet, der Benutzer erstellt ein Backup seiner wichtigsten Daten oder besser noch seines gesamten Systems auf ein externes Speichermedium, welches er anschließend vom PC trennt. Bei einer Infektion mit einem Verschlüsselungstrojaner wie z. B. Locky werden in der Regel sämtliche Dateien auf dem Rechner verschlüsselt. Gegen Zahlung eines Lösegelds in Form von Bitcoin verspricht der Angreifer dem Benutzer dann eine Entschlüsselung seiner Daten. Darauf sollten Sie aber niemals eingehen, da weder sichergestellt ist, dass die Daten überhaupt wieder entschlüsselt werden, noch sichergestellt ist, dass der Schadcode vom Rechner verschwindet und die Daten am nächsten Tag nicht wieder verschlüsselt sind. Besitzt der Benutzer allerdings eine Offline-Kopie seiner Daten, kann er den PC neu aufsetzen und seine Daten wieder zurückspielen.
Als dritte Maßnahme empfehle ich zum sehr vorsichtigen Umgang mit E-Mails, insbesondere wenn diese Links zu anderen Webseiten oder Dateianhänge besitzen. E-Mail ist das Einfallstor Nr. 1, wenn es um Cyberangriffe geht. Bei Erhalt einer E-Mail sollte der Benutzer sich immer folgende Fragen stellen „Kenne ich den Absender und kann ich verifizieren, dass er das auch wirklich ist?", „Erwarte ich diese E-Mail (insbesondere von diesem Absender)?" und „Erwarte ich diesen Anhang/diesen Link in der E-Mail?". Kann ich eine oder mehrere dieser Fragen mit „Nein" beantworten, sollte ich die Mail auf keinen Fall öffnen und im Zweifelsfall einen Nachweis über die Identität des Absenders sowie die Echtheit der Mail bei diesem fordern, möglichst unter Verwendung eines zweiten Kommunikationskanals (z. B. via Telefon, Messenger, etc.).
Als vierte und letzte Maßnahme rate ich zum grundsätzlichen Misstrauen im Internet. Verstehen Sie mich bitte nicht falsch, meiner Meinung nach ist das Internet einer der wichtigsten Errungenschaften der Menschheit und bietet uns unendliche viele Chancen, wie etwa weltweite Kommunikation und Datenaustausch in nahezu Echtzeit, was wesentlich zur Steigerung unserer Lebensqualität beigetragen hat. Aber es ist gleichzeitig eine Art Paradies für Kriminelle, die sich an anderen Menschen mit weniger Kenntnissen in diesem Bereich bereichern wollen. Besonders die Möglichkeit, seine wahre Identität relativ einfach verschleiern zu können, eröffnet den Kriminellen im Internet zahlreiche Möglichkeiten. Daher sollten Benutzer bei sämtlicher Kommunikation im Internet stets misstrauisch sein und anderen Akteuren mit einer gewissen Skepsis begegnen, bis deren Identität zweifelsfrei bestätigt und die Kommunikation geschützt von statten gehen kann.

**Konrad-Adenauer-Stiftung:**
Bietet die Krise vielleicht auch die Chance über Cybersicherheit aufzuklären, da sich viele gezwungenermaßen auf Arbeit oder Sozialleben im Netz einstellen mussten?

**Jonas Grasediek:**
Aus meiner Sicht bietet die Krise definitiv die Chance das Thema Cybersicherheit nochmal in den Fokus zu rücken. Und das ist in der aktuellen Situation auch notwendig, da Cyberkriminelle diese gezielt für ihre Machenschaften ausnutzen. Meine bisherige Erfahrung ist, dass in vielen Firmen das Thema Cybersicherheit eher als ein notwendiges Übel betrachtet wird, dem kein ausreichend hoher Stellenwert zukommt.
Spätestens seit Beginn der Krise hat das Thema Home-Office hingegen einen sehr hohen Stellenwert eingenommen und es gibt Firmen, die an dauerhaften oder zeitweisen Home-Office-Modellen für ihre Mitarbeiter arbeiten. Für deren korrekte und sichere Umsetzung benötigt man allerdings ein entsprechendes Sicherheitskonzept, das auch die umfängliche Sensibilisierung aller Mitarbeiter zum Thema Cybersicherheit beinhaltet. Daraus ergibt sich sowohl für Unternehmen als auch deren Mitarbeiter die große Chance, das Thema Cybersicherheit deutlich umfangreicher zu betrachten als es bisher der Fall war. Der Bedarf nach mehr Aufklärungsarbeit ist auf jeden Fall vorhanden und sollte von den entsprechenden Verantwortlichen wahrgenommen und gedeckt werden.

**Konrad-Adenauer-Stiftung:**
Gibt es weitere Literaturempfehlungen für Nutzer, die sich intensiver mit dem Thema beschäftigen möchten?

**Jonas Grasediek:**
Zum Thema Cybersicherheit existiert prinzipiell eine Vielzahl an Literatur. Die Frage ist, wie tief der Nutzer sich jeweils mit der Thematik beschäftigen möchte.
Grundsätzlich empfehle ich die Webseite „BSI für Bürger" des Bundesamtes für Sicherheit in der Informationstechnik. Diese richtet sich in erster Linie

an Nutzer ohne tiefgehende IT-Kenntnisse und bietet u. a. die Möglichkeit sich grundlegende Begrifflichkeiten im Kontext der Cybersicherheit verständlich erläutern zu lassen. Des Weiteren können Nutzer sich hier auch über aktuelle Geschehnisse und Risiken durch Cyberkriminalität informieren und bei Bedarf einen Newsletter abonnieren, um regelmäßig Hinweise zu aktuellen Schadcode-Kampagnen und Patches zu erhalten. Zudem besitzt das BSI auch einen eigenen YouTube-Kanal, auf dem verschiedene Themen wie etwa das Verschlüsseln von E-Mails oder auch die Zwei-Faktor-Authentifizierung leicht verständlich erläutert werden. In meiner Präsentation zum Webinar habe ich bewusst immer wieder auf das BSI für Bürger referenziert, da ich es besonders für den Durchschnittsnutzer als eine sehr gute Quelle erachte.

YouTube würde ich auch generell als Quelle empfehlen, da es hier viele Kanäle gibt, die Begrifflichkeiten und Themen aus dem Bereich Cybersicherheit sowie deren Zusammenhänge gut verständlich erklären. Meist reicht es schon aus, einen Suchbegriff wie z. B. „E-Mails verschlüsseln mit PGP" in die Suchzeile einzugeben, um mehrere Videos mit jeweils ca. 3 bis 6 Minuten Laufzeit zu erhalten, die das entsprechende Thema erläutern.

Wer sich sehr tief mit der Materie auseinandersetzen möchte, dem empfehle ich Bücher wie „Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen", „Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung" sowie „Netzsicherheit: - Grundlagen & Protokolle - Mobile & drahtlose Kommunikation - Schutz von Kommunikationsinfrastrukturen". Für Nutzer, die sich zunächst grundlegenden Themen wie Informatik, Rechnernetze und den eigentlichen EDV-Grundlagen annehmen wollen, denen sei das „IT-Handbuch für Fachinformatiker" empfohlen. Es handelt sich hierbei um ein Lehrbuch, welches ich stets Auszubildenden und Studenten empfehle, die die Grundlagen verschiedener IT-Themen erlernen wollen.

Den Nutzern die am Webinar teilgenommen haben, möchte ich abschließend noch die von mir zur Verfügung gestellte Linkliste empfehlen. Diese enthält Links zu allen von mir im Webinar vorgestellten Themen und Konzepten und soll als Nachschlagewerk dienen.

Das Interview fand Mitte Juni 2020 statt.
Die Fragen stellte Christian Kutzscher.

**Konrad-Adenauer-Stiftung e. V.**
**Christian Kutzscher**
Studentische Hilfskraft Politisches Bildungsforum Rheinland-Pfalz
Politische Bildung
Weißliliengasse 5
55116 Mainz
www.kas.de/rp

christian.kutzscher@kas.de
kas-rp@kas.de