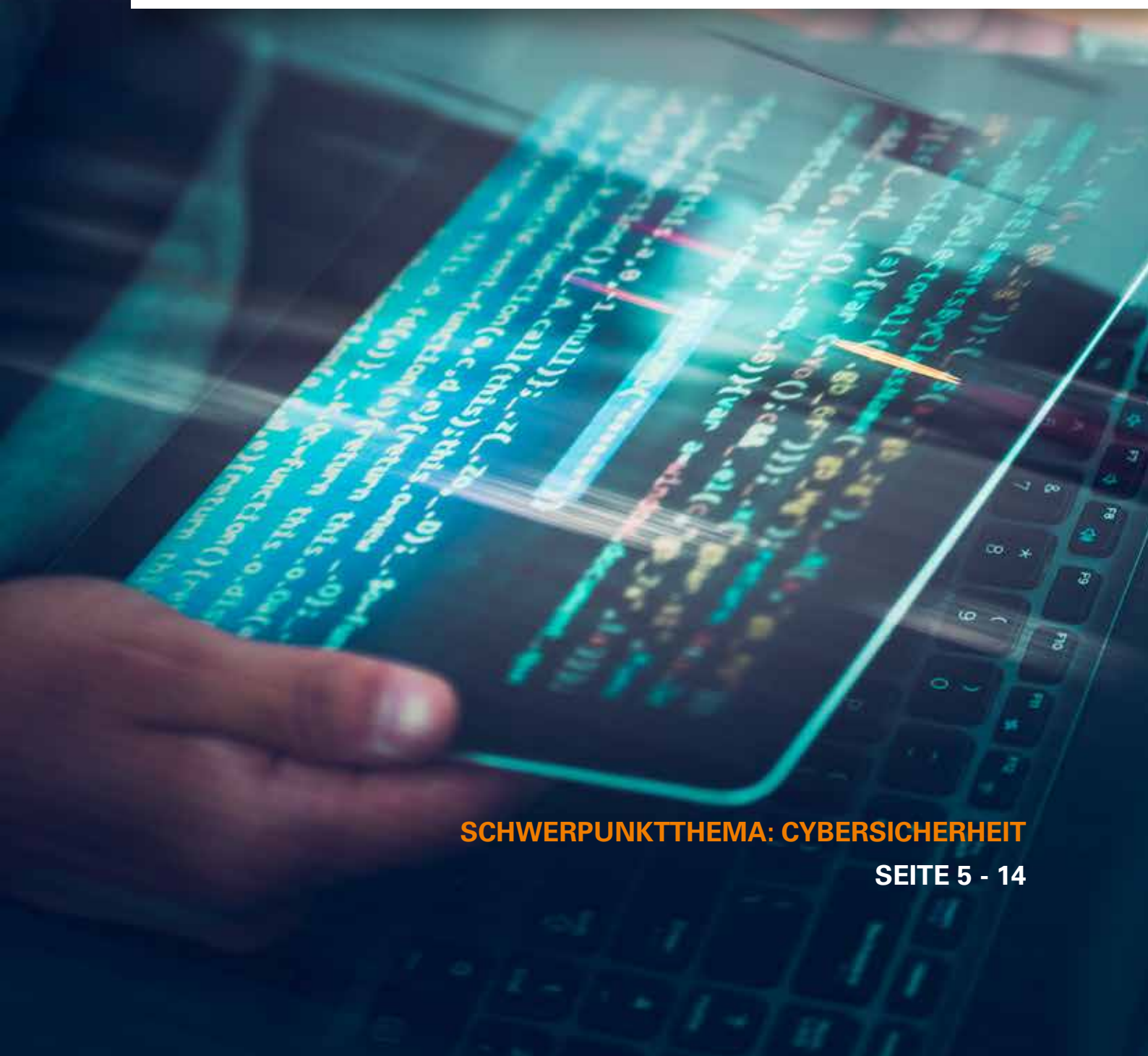




Ausgabe 01 | 2022

# DAS ZUKUNFTSMAGAZIN

ZENTEC



**SCHWERPUNKTTHEMA: CYBERSICHERHEIT**

**SEITE 5 - 14**

Mit freundlicher Unterstützung von



## Impressum

ZENTEC GmbH  
Zentrum für Technologie, Existenzgründung  
und Cooperation  
Industriering 7  
63868 Großwallstadt

Telefon: 06022 26-0  
Telefax: 06022 26-1111  
E-Mail: [redaktion@zukunfts magazin.de](mailto:redaktion@zukunfts magazin.de)  
Internet: [www.zukunfts magazin.de](http://www.zukunfts magazin.de)

Redaktion & Anzeigenbetreuung:  
Thorsten Stürmer, Marc Gasper

ISSN-Nr.: 1862-1104  
Auflage: 2000  
Bezug kostenlos

<b>I</b>	<b>Inhalt</b>	<b>3</b>
<b>II</b>	<b>Editorial</b>	<b>4</b>
<b>III</b>	<b>Schwerpunktthema: Cybersicherheit</b>	<b>5</b>
	Homeoffice und Cyberangriffe, wie passt das zusammen? .....	5
	IT-Security-Vortragsreihe wird 2022 fortgesetzt .....	7
	Sicherheit in IT-Netzwerken des Mittelstands.....	9
	Business Continuity Management als Hands-on-Ansatz .....	11
	Cyber-, Informations- & IT-Sicherheit – alles das Gleiche? .....	13
<b>IV</b>	<b>Das Zukunftsmagazin im Interview mit Reinald Kempf, Geschäftsführer der echoway GmbH</b>	<b>15</b>
<b>V</b>	<b>Neuigkeiten aus der Region</b>	<b>19</b>
	Transformationssprechtage für Unternehmen am Bayerischen Untermain.....	19
	Mentor und Sparringspartner: ASC unterstützt Start-up-Inkubator .....	20
	Der neue UV-Luftreiniger Soluva Air F ist gleichzeitig leicht, leise und leistungsstark .....	21
	Weiterbildung zum Betrieblichen Pflegeleitenden/zur Betrieblichen Pflegeleiterin findet auch 2022 wieder statt .....	22
	Unternehmensstrategie: C+ITEC AG wird zu Firstcom Europe AG.....	22
	Beginn des neuen Förderprojekts „Weiterbündelungsverband (Automotive) Bayerischer Untermain“.....	23
	Arbeitnehmer und Arbeitgeber voranbringen: Das Projekt „Weiterbündelungsverband“ am Bayerischen Untermain geht weiter bis Ende 2024! .....	24
	Theo Klein + Partner feiert 30-jähriges Firmenjubiläum.....	25
<b>VI</b>	<b>Stimmen aus der Politik</b>	<b>27</b>
	Cyberangriffe auf die öffentliche Verwaltung – welche Gefahr besteht für bayerische Kommunen?....	27
	Bayern stärkt die Cybersecurity .....	29
<b>VII</b>	<b>Kolumne zum Schluss</b>	<b>31</b>

### Liebe Leserinnen und Leser,

„dreist, aber gar zu durchsichtig“, war unser erster Gedanke dieser Tage, als das BSI – Bundesamt für Sicherheit in der Informationstechnik – wieder eine neue Gefahrenmeldung herausgab: „Mit Bezug zum russischen Angriffskrieg gegen die Ukraine sind nun auch betrügerische E-Mails im Namen von Banken im Umlauf. Die Kriminellen geben bspw. vor, dass man kontrollieren müsse, ob sich die Kundinnen und Kunden an Sanktionen halten. Dabei handelt es sich in jedem Fall um Phishing-Versuche!“ Doch gibt es sicher wieder mehr als genug Menschen, die auf diese Mails hereinfliegen, weil ... sie überarbeitet, gutgläubig, unaufmerksam, ängstlich etc. sind. Und mit der Angst der Menschen lässt sich bekanntlich ja eh gut spielen.

Wer kann auch den Überblick behalten bei 394.000 neuen Schadprogrammvarianten pro Tag? So hoch ist nämlich laut BSI-Lagebericht vom Oktober 2021 der Durchschnitt der erfassten Varianten. Rechnet man das auf ein Jahr hoch sind das satte 144 Millionen.

Das Geschäft mit der Datensicherheit bzw. Datensicherheit ist ein Großes. Auf der einen Seite die „Bösen“, die mit Lösegeldforderungen, Schutzgeld-erpressung und Spionage die Unternehmen und den Staat um Milliardenbeträge erleichtern. Auf der anderen Seite die, die das Böse für den guten Zweck simulieren und Systeme sichern, und so ihre Kundschaft vor dem Eintritt des Wahrscheinlichen bewahren möchten. Kosten für Hardware, Software, Awareness-Trainings, – all dies müssen deutsche Unternehmen und Institutionen aufbringen, um einigermaßen sicher zu sein. Da gilt es eine gute Wahl in Bezug auf den IT-Dienstleister zu treffen.

Einige davon stellen wir Ihnen heute in unserem Z! Das Zukunftsmagazin vor. Auch finden Sie wieder eine Reihe von interessanten Neuigkeiten aus der Region. Wir wünschen eine inspirierende Lektüre.

Ihre Redaktion Z! Das Zukunftsmagazin

## Wussten Sie schon...

- ... dass der Abschuss-Code für US-Atomwaffen mehr als 20 Jahre lang 00000000 lautete?
- ... dass ein Universitätsklinikum nach einem Ransomware-Angriff 13 Tage lang keine Notfallpatienten aufnehmen konnte?
- ... dass die gängige Annahme, dass Digital Natives besser für Cyber Angriffe gerüstet sind als ältere Generationen, falsch ist? Durch ihr laxes Verhalten in den Sozialen Medien sind sie leichte Opfer.
- ... dass die Bezeichnung für weibliche Händer Hacker ist?



**SCHWERPUNKTTHEMA:**

**CYBERSICHERHEIT**

## Homeoffice und Cyberangriffe, wie passt das zusammen?

Da braucht es keine lange Recherche oder keine intensive Aufklärungsarbeit. Jeder, vom kleinen Einmannbetrieb über den Mittelständler bis hin zum Konzern, weiß über die Gefahren, die die Digitalisierung mit sich bringen kann. Eine Befragung des Kriminologischen Forschungsinstitut Niedersachsen e. V. in 2020 ergab, dass 59,6 % der insgesamt 687 befragten Unternehmen mindestens zweimal in den letzten 12 Monaten (2018/19) Cyberangriffen ausgesetzt waren. Meist sahen sich die Unternehmen mit Phishing-Angriffen, Ransomware und Spyware konfrontiert.

Cyberangriffe sind anhand vieler weiteren Erhebungen durch wichtige Institute als große Bedrohung für Unternehmen erkannt worden. Die Bitkom schreibt am 5. August 2021 gar von mehr als 220 Milliarden Euro Schaden pro Jahr für die deutsche Wirtschaft.

Die MitarbeiterInnen stellen hier eine zentrale Rolle dar. Sie sind oftmals der Gatekeeper, die primäre Firewall gegen Cyberangriffe. Nur wenn die Beschäftigten sensibel auf Angriffe reagieren, die firmenintern eingeleiteten Maßnahmen annehmen und entsprechend umsetzen, können diese erfolgreich abgewehrt werden.

### Welche Rolle spielt bei den Hacker-Angriffen das Kommunikationssystem?

Auf den Servern des Kommunikationssystems liegen zwar keine sensiblen Daten wie Bankkonten, Kreditkartennummern oder Geschäftsgeheimnisse, dennoch können erfolgreiche Angriffe einen immensen Vertrauensverlust für die betroffenen Firmen bedeuten. Die Daten, die auf Servern des Kommuni-

kationssystems erbeutet werden können, sind beschränkt auf Namen, Rufnummern, E-Mail-Adressen und teilweise auch Fotos. Die durch den Datendiebstahl betroffenen Kunden, können dann jedoch wiederum Angriffsopfer für Phishing-Nachrichten der Hacker werden.

Bei Hackern beliebt und bei Firmen gefürchtet, sind die sogenannten Fraud-Attacken oder Spoofing. Dabei telefonieren die Hacker auf Kosten ihrer Opfer. Sie dringen in die Telefonanlagen ein und verursachen durch Anrufe an kostenpflichtige Rufnummern – oft im Ausland – hohe Schäden. Neben einem geeigneten Passwortschutz, dem Einrichten von Sperrlisten und den regelmäßigen Updates kann ein professionelles Monitoring der Telefonsysteme helfen, Schäden zu minimieren oder gar komplett abzuwenden.

### Was ist das größte Einfallstor für die Angreifer?

So banal es klingen mag, aber nach wie vor verschaffen sich die meisten Angreifer Zugang über nicht aktualisierte Systeme. Gerade Software, die

mit dem Internet eine direkte Verbindung haben wie Router, Firewalls oder auch SBCs sind Ziel der Hacker. Werden die von den Herstellern zur Verfügung gestellten Patches nicht zeitnah eingespielt, öffnen sich die Türen für Angreifer, die diese Einladung nur zu gerne annehmen.

### Wie hoch ist die Bedrohung durch Cyberattacken auf Homeoffice-Mitarbeiter und deren Geräte einzuschätzen?

In einer repräsentativen Studie des Digitalverbands Bitkom gaben 59 % der befragten Unternehmen an, seit Beginn der Pandemie habe es IT-Sicherheitsvorfälle gegeben, die auf die Heimarbeit zurückzuführen seien. In 24 % dieser Unternehmen sei das sogar häufig geschehen. Sofern ein Angriff mit dem Homeoffice in Verbindung stand, ist daraus in der Hälfte der Fälle (52 %) auch ein Schaden entstanden. Achim Berg, Bitkom-Präsident drückt es so aus: *„Mitarbeiterinnen und Mitarbeiter einfach zum Arbeiten nach Hause zu schicken, genügt nicht. Ihre Geräte müssen gesichert, die Kommunikationskanäle zum Unternehmen geschützt und die Belegschaft für Gefahren sensibilisiert werden. Wer das nicht tut, verhält sich fahrlässig.“*<sup>1</sup>

Gerade die Homeoffice-Mitarbeiter können ein Einfallstor für Hacker sein. Eher isoliert arbeitende MitarbeiterInnen im Homeoffice öffnen tendenziell öfter gefälschte Mails oder die Software für Teamkommunikation hat Schwachstellen. Meist sind private Firewalls anfälliger als ein Firmennetzwerk.

### Was empfehlen die Experten der Firstcom Europe gegen den Datenklau?

Felix Seban, Service Manager der Firstcom Europe, hat hierzu ein klares Statement: *„Das Wichtigste ist immer noch gesunder Menschenverstand. MitarbeiterInnen, die wachsam sind und nicht auf Links klicken, die sie nicht kennen, sind noch immer der beste Schutz! Natürlich bieten wir auch Monitoring an und erkennen daher schnell Angriffe auf die uns anvertrauten Systeme. Aber auch das ausgeklügeltste Monitoring versagt, wenn der Faktor Mensch das Einfallstor öffnet. Niemand kann sich vor dieser Verantwortung wegducken. Schulungen und das Sensibilisieren der Belegschaft für die Angriffe ist dabei das A und O.“*

### Wie sicher oder unsicher sind Cloud Telefonsysteme?

Durch die hohen Sicherheitsmaßnahmen des Rechenzentrums ist die Universe-Cloud, die Cloud-Te-

lefonanlage der Firstcom Europe, bestens geschützt. In einem TÜV zertifiziertem High Performance Rechenzentrum in Frankfurt am Main sind die Telefoniefunktionen gehostet. Alle Daten sind mit höchstmöglichem Sicherheitsstandard durch Firewall und Session Border Controller gegen Cyberattacken und Angriffe von Viren und sonstiger Ransomware geschützt. Zudem sind die Server gegen Stromausfall, Wasser- und sonstigen Schäden abgesichert. ■

#### So schließen Sie die Schlupflöcher Ihrer Telefonanlage für Angreifer:

- Die voreingestellten PIN der Telefonanlage und der Sprachboxen ändern
- Für den Zugang mit Fernwartung sollte es klare Sicherheitsregeln geben
- Nicht benötigte Nebenstellen sollten grundsätzlich abgeschaltet werden, ebenso nicht benötigte Voicemail-Boxen
- Neue Softwareversionen (Patches) müssen zeitnah eingepflegt werden
- Rufnummersperren einrichten
- Monitoring regelmäßig auf Auffälligkeiten überprüfen

#### Maßnahmen, die die Gefahren der verteilt arbeitenden Teams minimieren?

- Virens Scanner auch im Homeoffice immer aktuell halten
- Möglichst über Terminalserver arbeiten
- Erstellen von schriftlichen Richtlinien zur Informations- und IT-Sicherheit
- aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates
- Auslagerung der IT-Security an externe Dienstleister

## Ansprechpartner

Andreas Herget  
Firstcom Europe AG  
Dammer Weg 51  
63773 Goldbach  
06021 4436-1100  
vertrieb@firstcomeurope.de  
www.firstcomeurope.de

<sup>1</sup> <https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr>

## IT-Security-Vortragsreihe wird 2022 fortgesetzt

„IT-Security für die Region, aus der Region.“ Unter diesem Motto findet seit 2020 die Vortragsreihe, welche im Verbund zwischen dem Digitalen Gründerzentrum Alte Schlosserei (DGZ), der IHK Aschaffenburg und ExpertInnen aus der Region veranstaltet wird, statt. Auch in diesem Jahr gibt es wieder zwei Veranstaltungen, an denen Unternehmen sich zu den Themen „Netzwerksicherheit“ und „Mobile Devices“ informieren und beraten lassen können.

Die Digitalisierung bietet für Unternehmen viele Vorteile – Prozesse werden verbessert, Kosten eingespart und neue Geschäftsmodelle erschlossen. Aber die zunehmende Technologisierung der Wirtschaft birgt auch Risiken. Cyberangriffe, Datenpannen und Systemausfälle können Unternehmen schweren Schaden zufügen. Die Bedrohungen werden dabei immer vielseitiger und werden oft erst erkannt, wenn Systeme bereits angegriffen oder ausgefallen sind. Insbesondere Angreifer (Hacker) finden immer neue Möglichkeiten, sich illegal Zutritt zu Unternehmenskonten zu verschaffen. Erst im vergangenen November kam es beispielsweise zu einem Angriff auf die MediaMarkt-Saturn-Gruppe, welcher tagelange Störungen der Kassensysteme und vieler Services zur Folge hatte. „Cyberkriminelle haben längst auch mittelständische Unternehmen als lohnendes Angriffsziel ausgemacht. Neben beträchtlichen Erpressungszahlungen gehen die Angriffe dabei auch vielfach mit einem Verlust von Know-how oder dem Stillstand der Produktion einher“, so Andreas Elsner, Bereichsleiter Innovation & Umwelt, IHK Aschaffenburg.

Im dauernden Wettstreit der Weiterentwicklung von IT-Sicherheit und Schadsoftware ist es zunehmend schwer, das eigene Unternehmen vor den Gefahren zu schützen. „Um dem entgegenzuwirken, haben wir diese Veranstaltungsreihe ins Leben gerufen. Das Know-how von Expertinnen und Experten soll gezielt an die Unternehmen im Mainviereck weitergegeben werden, um für die Risiken zu sensibilisieren und Wege aufzuzeigen, wie man MitarbeiterInnen und das Unternehmen vor Angriffen schützen kann“, so Dr. Marianne Hock-Döpgen, Leiterin des DGZ. Die Expertinnen und Experten stammen dabei aus der Region und bieten ihre Vorträge kostenfrei an. So beteiligen sich neben dem DGZ, die IHK Aschaffenburg und der Kriminalpolizei auch die Unternehmen Applied Security, Peter Communication Systems, Protektis, InTo Consulting und das Startup MainDefense an dieser Vortragsreihe.



Digitales Gründerzentrum Alte Schlosserei

„Als wir auf das Vorhaben angesprochen wurden, waren wir sofort dabei, denn aus unserer Sicht steigert der ganzheitliche Blick auf das Thema IT-Sicherheit die Resilienz der Unternehmen und ist ein wichtiger Beitrag zur Digitalen Transformation der regionalen Wirtschaft“, sagt Matthias Peter, Geschäftsführer von Peter Communication Systems. „Für uns als IT-Systemhaus ist es eine Daueraufgabe, unseren hauptsächlich mittelständischen Firmenkunden praktische Unterstützung in Sachen IT-Sicherheit zu leisten.“

Seit 2020 findet die Vortragsreihe „IT-Security für die Region“ unter wechselnden Themenschwerpunkten statt. Dabei werden komplexe Themen der IT-Sicherheit aufbereitet und verschiedene Vorträge geben interessierten Unternehmen und Start-ups einen Überblick über die verschiedenen Bereiche der Angriffs- und auch Schutzmöglichkeiten wieder. Die Vorträge richten sich dabei nicht nur an IT-SpezialistInnen, sondern an alle UnternehmerInnen, die mehr über IT-Sicherheit erfahren möchten. „Viele

Schwerpunktthema: Cybersicherheit

Unternehmen sind verunsichert, wie sie sich gegen Angriffe effektiv absichern können und fühlen sich teilweise sogar machtlos gegen die wachsenden Bedrohungen. Durch die Vorträge können wir Wege aufzeigen, wie man sich als UnternehmerIn effektiv absichern kann,“ erklärt Frank Schlotzke, Geschäftsführer von Applied Security.

Passend zu den Herausforderungen durch die Corona-Pandemie wurden in den bisherigen Vorträgen Themen wie „Homeoffice“ und „Mitarbeiter-Awareness“ besprochen, denn viele Unternehmen mussten innerhalb kürzester Zeit die Mitarbeitenden in die Heimarbeit schicken, ohne ausreichend Zeit gehabt zu haben, sich mit dem Thema der IT-Sicherheit zu befassen.

Auch in 2022 wird die erfolgreiche Reihe fortgesetzt. Die nächste Veranstaltung findet am 31.05.2022 im Digitalen Gründerzentrum „Alte Schlosserei“ statt. Zu dem Themenschwerpunkt „Netzwerksicherheit“

werden Kriminalhauptkommissar Oliver Weidel, Matthias Peter (Peter Communication Systems), Frank Fengel (Protektis) und Ines Toth-Strichirsch (InTo Consulting) berichten. ■

Informationen und Anmeldung unter: [dgz-ab.de/event](http://dgz-ab.de/event)

## Ansprechpartner

Florian Zschka  
Digitales Gründerzentrum Alte Schlosserei  
Werkstr. 2  
63739 Aschaffenburg  
06021 391-377  
[florian.zschka@dgz-ab.de](mailto:florian.zschka@dgz-ab.de)  
[www.dgz-ab.de](http://www.dgz-ab.de)

# DIGITALES GRÜNDERZENTRUM ALTE SCHLOSSEREI - ASCHAFFENBURG



KOMM  
ZU UNS

## DU HAST DIE IDEE?

Fragst dich aber, was du als nächstes tun sollst und wie du die Idee umsetzen kannst?

Dann komm zu uns! Wir bieten dir: • Beratung • Mentoring • Coachings • Workshops • Vorträge • Workspaces

[www.dgz-ab.de](http://www.dgz-ab.de)

• Netzwerk • Finanzierungs- und Fördermöglichkeiten





## Sicherheit in IT-Netzwerken des Mittelstands

**Welche technischen Maßnahmen bieten noch Schutz gegen moderne Angriffe oder verbessern die IT-Sicherheit? Zurecht wird in aktuellen Konzepten zur Vermeidung von Angriffen auf IT-Netzwerke der Anwender in den Fokus der Bemühungen gerückt. Awareness-Trainings, Phishing-Simulationen usw. helfen gerade auch Nicht-ITlern, z. B. verdächtige E-Mails zu erkennen und richtig zu reagieren. Dabei vermittelt der umfassende Einsatz von Cloud-basierten Diensten eine eventuell trügerische Sicherheit, wenn lokale Sicherheitsüberlegungen außer Acht gelassen werden.**

Aber welche technischen Maßnahmen verbleiben für Administratoren mittelständischer Unternehmen, um einen angemessenen Schutz der IT zu gewährleisten und die AnwenderInnen im Netzwerk zu unterstützen? Funktionierende Backups, wirksame Antivirus-Lösungen und Next Generation Firewalls dürfen in den meisten Netzwerken als bereits vorhandene Mindeststandards angenommen werden. Einige Gefahren für die Verfügbarkeit von IT-Systemen rühren gar nicht von Hacker-Angriffen her, sondern wirken direkt auf die physische Sicherheit, so z. B. Diebstahl, Beschädigung, Feuer, Wasser, Staub, Temperatur und Luftfeuchtigkeit etc.

### Zutritt und Umgebungsparameter überwachen

Nicht nur, wo noch lokale Serversysteme gegeben sind, sondern auch dort, wo andere schützenswerte Netzwerkkomponenten vorhanden sind, wie z. B. zentrale Switches, Router und Backup-Lösungen, sollte dringend für die Überwachung der Umgebungsparameter der betreffenden Räume gesorgt werden.

Einen wichtigen Anfang stellen gegen unbefugten Zutritt geschützte Räume und Netzwerkschränke dar. Ein elektronisches Zugangskontrollsystem stellt z. B. sicher, dass die Türöffnung nur mit einer elektronischen Autorisierung (RFID-Karte oder -Anhänger, PIN-Eingabe etc.) erlaubt ist und die Zutritte dokumentiert werden. Eine daran angeschlossene intelligente Videoüberwachung liefert zusätzlich den Bildnachweis, dass die verwendeten Zutrittsmedien auch von den erwünschten Personen verwendet werden.

Peter Communication Systems stattet die Räume und Schränke mit Systemen aus, die die Überwachung von Raumbedingungen wie Temperatur, Luftfeuchtigkeit, Staubbelastung, Raumluft, Erschütterung und weiterer Parameter erlauben. Diese

warnen bei Abweichungen von den definierten Sollwerten z. B. per Anruf, SMS und/oder E-Mail. So können z. B. Brände vermieden werden, lange bevor es zu Rauchentwicklung oder offenem Feuer kommt.

Darüber hinaus gibt es noch weitere sinnvolle Hardware- und Software-Lösungen, die den AnwenderInnen die „Awareness“ zwar nicht abnehmen, aber zumindest einige erkennbare Angriffsmuster aufdecken oder anderweitig helfen, die Sicherheit zu verbessern. Glücklicherweise wird z. B. eine Zwei-Faktor-Authentifizierung von vielen Anwendungen inzwischen zwingend vorausgesetzt, aber es bleiben noch offene Handlungsfelder.

### Schwache Passwörter und schlechtes Passwort-Management als Risiko

Firmenrichtlinien, die die Verwendung starker Passwörter und deren regelmäßige Änderung verlangen sowie die Mehrfachnutzung von Passwörtern verbieten, stellen nur einen frommen Wunsch dar, wenn den AnwenderInnen keine praktische Hilfe geleistet wird, diese auch umzusetzen.

Um dieser Herausforderung zu begegnen, empfiehlt Peter Communication Systems den Einsatz einer Passwort- und Identitätsmanagementlösung. Diese erlaubt es, eben nicht nur der IT-Abteilung(!), Passwörter sicher zu wählen und zu verwahren sowie leicht aufzufinden und zu verwenden. Nebenbei werden Änderungen und die Verwendung der Passwörter dokumentiert, sowie Urlaubs- und Krankheitsvertretungen realisiert.

Die Planung und Einführung einer solchen Lösung über ein ganzes Unternehmen stellt zwar einmalig einen gewissen Aufwand dar, dieser zahlt sich aber langfristig durch die Verbesserung der Benutzerakzeptanz zur Verwendung sicherer Passwörter aus.





Beispiele für technische Maßnahmen zur Überwachung und zum Schutz von Serverräumen und -Schränken (Quelle: Kentix GmbH)

### Technische Verbesserungsmöglichkeiten im Umgang mit E-Mails

In vielen Umgebungen werden die Mails unzureichend gegen Mitlesen auf dem Übertragungsweg geschützt und offensichtlich erkennbare Spam- und Malware-Inhalte werden zu selten erkannt. Hier besteht immer noch dringender Handlungsbedarf bezüglich der sicheren Verwendung von E-Mails.

Dabei gibt es effiziente Lösungen zur Erkennung unerwünschter Inhalte, die weit über die Funktionen der von Haus aus in Mailanwendungen integrierten Filter hinausgehen. Die Kombination verschiedener, intelligenter Filter bietet ein weit höheres Detektions- und Schutzniveau, sodass potenziell gefährliche Mails gar nicht erst in das Postfach der jeweiligen NutzerInnen zugestellt werden.

Dies wird idealerweise kombiniert mit einer tatsächlich einfach zu bedienenden Verschlüsselung von Mails, die den gesamten Übertragungsweg vom Absender bis zum Empfänger zuverlässig vor Mitlesen und Manipulation der Inhalte schützt. ■

### Ansprechpartner

Matthias Peter  
Peter Communication Systems GmbH  
Benzstraße 2A  
63741 Aschaffenburg  
06021 3709-14  
mpeter@peter-cs.de

## Business Continuity Management als Hands-on-Ansatz

**Die vergangenen zwölf Monate haben deutlich gezeigt, wie schnell unvorhergesehene Ereignisse die Geschäftsprozesse eines Unternehmens erheblich stören und ernsthafte Schäden oder vernichtende Verluste verursachen können. Lockdowns der Wirtschaft, Verpflichtung zum Homeoffice, Massenerkrankungen der Belegschaft, aber auch massive Angriffe auf die IT der Unternehmen in Form von Datenspionage oder Hackerangriffe sind nur einige Beispiele.**

Wer in solchen Fällen auf ein professionelles Krisenmanagement bzw. ein „Betriebliches Kontinuitätsmanagement“ zugreifen kann, ist hier im Vorteil. „Betriebliches Kontinuitätsmanagement“, auf Englisch Business Continuity Management (BCM), hat das Ziel, Schäden von Unternehmen zu minimieren und bestmögliche Vorkehrungen für den Fall gravierender Störungen zu treffen. Das BCM-System definiert Pläne, wie der reguläre Betrieb nach störungsbedingter Unterbrechung in kürzest möglicher Zeit wieder aufgenommen werden kann. So lassen sich Schäden reduzieren und existenzielle Bedrohungen für das eigene und verbundene Unternehmen vermeiden.

### BCM nach ISO 22301

Die internationale ISO 22301 Norm hilft, die wichtigsten Punkte für ein Business Continuity Management zu berücksichtigen. Sie schafft das Verständnis und liefert den geeigneten Rahmen für die Implementierung eines BCM-Systems in Unternehmen jeder Branche und Größe. Wie alle anderen Anforderungen an Managementsysteme fordert die ISO 22301 grundsätzliche Dinge wie Verfahren, die den systematischen Betrieb organisationsindividuell festlegen.

Der Nachteil der Einführung eines BCM-Systems nach ISO 22301 ist die Komplexität. Kernelemente wie die Business Impact Analyse (BIA) und das Risiko Assessment müssen zwingend umgesetzt werden. Erst nach der theoretischen Analyse erfolgt die praktische Umsetzung im Rahmen von Business Continuity Aktivitäten. Die meist für BCM-Systeme nach ISO 22301 erforderlichen Werkzeuge und Berater stellen zudem einen enormen Kostenfaktor dar, den so mancher Mittelständler scheut. Dadurch bleiben die Beschäftigung mit Risiken und die Einführung eines BCM leider oft komplett auf Strecke.

### Der pragmatische Hands-on-Ansatz


Abgeschreckt vom Aufwand, ist gar nichts tun jedoch

die falsche Strategie. Denn ein BCM ist nahezu für jedes Unternehmen überlebenswichtig. Nüchtern betrachtet, handelt es sich beim BCM um technische, organisatorische sowie personelle Maßnahmen im Unternehmen, um nach einem Krisenfall die Fortführung des Kerngeschäftes zu sichern.

Im Grunde muss auf Managementebene „lediglich“ festgelegt und niedergeschrieben werden, welche Vorkommnisse eine Beeinträchtigung des Betriebs darstellen und wie damit umgegangen werden muss. Damit wird sichergestellt, dass im realen Fall wertvolle Zeit gespart wird, weil die Planung in großen Teilen schon erledigt ist. Diese Vorarbeiten können ganz pragmatisch in einem einfachen Textdokument festgehalten werden, das anschließend gesichert abgelegt werden sollte. Für die tiefergehende Planung, Festlegung und Ausführung der Business Continuity Aktivitäten im Ernstfall gibt es IT-Systeme, die nur einen Bruchteil der professionellen BCM-Tools kosten. Idealerweise sollte solch ein System abgekoppelt von der Unternehmens-IT – also z. B. webbasiert als SaaS-Lösung – arbeiten. Das ist deshalb so wichtig, weil beispielsweise bei einem Cyberangriff zumeist die gesamte eigene IT-Infrastruktur runtergefahren wird. Als abgekoppelte IT-Lösung ist das BCM-System autark und erledigt in der Krisensituation zuverlässig seine Arbeit.

Wie Unternehmen mithilfe eines solchen pragmatischen BCM-Systems in der Krise entscheidungs- und handlungsfähig bleiben, zeigen die folgenden sechs Schritte. Diese verfolgen im Grundgedanken das Konzept des PDCA-Zyklus nach Demming (Plan-Do-Check-Act).

### Schritt 1: Durchdachte Krisenplanung

Ganz am Anfang steht der Plan (Plan). Dabei arbeitet man idealerweise mit verschiedensten Szenarien, die eine Krisensituation hervorrufen können. Die Zahl 

der möglichen Szenarien kann dabei beliebig groß sein und sollte zumindest alle halbwegs realistischen Krisensituationen abbilden. Hierzu zählen eigentlich immer IT-Pannen, Hackerangriffe, aber auch – wie im vergangenen Jahr mehrfach vorgekommen – Masenerkrankungen der Belegschaft, Umweltkatastrophen usw. Jedes Szenario erhält nun eine genaue Definition der eingebundenen Akteure sowie der notwendigen Maßnahmen im Rahmen von Reaktions- und Wiederanlaufplänen. Genaue Handlungsanweisungen legen fest, wer wann was wie zu tun hat.

### Schritt 2: Die Krise feststellen

Kommt es zu einer Krisensituation, sollten die notwendigen Maßnahmen schnell griffbereit sein (Do). Webbasierte Tools haben hier den Vorteil, dass die in der Planung vorbereiteten Maßnahmen jederzeit an jedem Ort verfügbar sind. So werden die im Plan genannten Akteure mobilisiert und können umgehend ihre Arbeit aufnehmen, um sich mit notwendigen Aktionen, der Ursachenanalyse und der Wiederherstellung des Normalzustandes zu befassen. Dies kann z. B. in einem definierten Krisenstab passieren oder für kleinere Vorkommnisse auch in der Hand einzelner Personen liegen. Damit möglichst schnell mit der Bearbeitung begonnen werden kann, empfiehlt es sich, die Mobilisierung der Akteure automatisiert durchzuführen, statt auf gedruckte Listen zu setzen, da diese immer die Gefahr bergen, veraltet zu sein.

### Schritt 3: Handlungsanweisungen ausführen

Die bereits vorbereiteten Handlungsanweisungen helfen bei der Schritt-für-Schritt-Abarbeitung des Krisenprozesses: zum Beispiel Schritte zur Ursachenanalyse, Verfassen einer Pressemeldung oder Wiederanlaufpläne für den Betrieb. Die Beschreibung der Einzelmaßnahmen hilft auch weniger erfahrenem Personal, die anfallenden Tätigkeiten nacheinander durchzuführen und zu dokumentieren. So entsteht bereits hier automatisch ein Überblick, wer wann und mit welchem Ergebnis Maßnahmen durchgeführt hat und welche noch zu erledigen sind.

### Schritt 4: Dokumentation und Informationsfluss

Neben der schnellen Reaktion und Lösung des Problems ist eine lückenlose Dokumentation der Erkenntnisse, Maßnahmen oder Hinweise besonders wichtig – nicht nur aus rechtlichen Gründen, sondern auch, um für die Zukunft die Szenarien weiter zu optimieren. Die Nachvollziehbarkeit und Auswertung der Maßnahmen zur weiteren Verbesserung decken damit den Punkt Check ab. Um diese notwendige chronologische Dokumentation bereits während der Arbeit erledigen zu können, sind sogenannte Einsatztagebücher (ETB) hilfreiche Instrumente. Diese

sollten so gestaltet sein, dass ein nachträgliches Ändern der Einträge nicht möglich ist. Neben der handschriftlichen Methode eignen sich dazu Systeme, die Einträge revisions sicher speichern. Digitale Lösungen bieten häufig den Vorteil, dass die Einträge allen Beteiligten direkt zur Verfügung gestellt werden können und so den Informationsfluss in der Krise signifikant verbessern.

### Schritt 5: Nachbesetzung

Sollte die Krise länger anhalten, kann eine Ablösung oder Erweiterung der aktuell Beteiligten erforderlich werden. Die frühe Beschäftigung mit dem Thema sorgt dafür, dass die Ablösung rechtzeitig eintrifft und der aktuelle Kenntnisstand geordnet übergeben werden kann. Vordefinierte Gruppen oder Schichten können helfen, diesen Prozess zu vereinfachen.

### Schritt 6: Aus dem Vorfall lernen

Wenn die Krisensituation im Griff ist und die Organisation wieder ihren Normalzustand erreicht hat, erfolgt die Nachbereitung, Analyse und ggf. Optimierung. Im PDCA-Zyklus wird die letzte Phase (Act) zur Reflexion genutzt. Sollten Optimierungspotenziale erkannt worden sein, wird das entsprechende Szenario beispielsweise bei den Akteuren oder Handlungsempfehlungen geändert oder ergänzt. An dieser Stelle helfen alle während der Krise angefertigten Aufzeichnungen.



### “Vor der Lage sein!”

Vor allem bei den Blaulichtorganisationen gibt es den Ausdruck “Vor der Lage sein!“. Gemeint ist, durch genügend Vorbereitung und Übung dem Geschehen immer einen Schritt voraus zu sein. Nur dann sind Unternehmen in der Lage zu agieren, anstatt zu re-

agieren. Genau das kann mit dem Hands-on-Ansatz erreicht werden, der sich bei konsequenter Anwendung schnell zu einem sinnvollen Maßnahmenkatalog entwickelt, der in der Praxis direkt angewendet werden kann.

Die webbasierte Plattform für Alarm- und Krisenmanagement GroupAlarm unterstützt effektiv dabei, Krisensituationen schnell und pragmatisch in den Griff zu bekommen. Das fängt bei der Planung an und hört mit der Dokumentation auf. Damit werden im Ereignisfall finanzielle Folgen reduziert und negative Auswirkungen auf die Reputation gemindert, denn eine Krise ist meist kostenintensiver als die Gegenmaßnahmen. ■

## Ansprechpartner

Hanno Heeskens  
 cubos Internet GmbH  
 Goethestraße 5  
 52064 Aachen  
 0241 56528880  
 vertrieb@cubos-internet.de  
 www.groupalarm.com

## Cyber-, Informations- & IT-Sicherheit – alles das Gleiche?

**Zumindest das Ziel teilen sich die Maßnahmen, die den drei Begriffen zuzuordnen sind, in jedem Fall: Immer geht es darum Unternehmenswerte, Daten, Systeme und Geschäftsprozesse zu schützen und sicherzustellen, dass der (IT-)Betrieb weiterläuft.**

Ob Produktion, Marketing, Vertrieb, Buchhaltung oder Personalwesen – heutzutage ist jede Abteilung IT-gestützt oder von IT abhängig. Bei dem Maß an Digitalisierung und dieser starken Abhängigkeit von IT-Systemen erübrigt sich die Frage, ob es Maßnahmen zur Absicherung braucht. Die Frage ist viel mehr: Wie viele und welche Maßnahmen sind notwendig?

Und diese Frage ist nicht ganz trivial zu beantworten, mehr geht nämlich immer. Sie können eine Firewall anschaffen oder ein Cluster bestehend aus mehreren. Sie können aber auch dieses Cluster noch redundant absichern und an einem zweiten Standort ein zweites Cluster aufstellen. Doch wieviel ist sinnvoll? Die wenigsten Unternehmen, gerade im (kleinen) Mittelstand haben unbegrenzte Budgets und es macht auch keinen Sinn zum Schutz von 10.000 Euro Bargeld einen Tresor zu kaufen der 50.000 Euro kostet.

### **Cybersicherheit darf kein Selbstzweck sein!**

Maßnahmen müssen zum Schutzbedarf des Unternehmens passen. Wichtig ist hierbei den Kontext der eigenen Organisation zu betrachten, darauf zu

achten, wie groß das Risiko für gewisse Gefährdungen anhand der Eintrittswahrscheinlichkeit und potenziellen Schadenshöhe tatsächlich ist und welche Maßnahmen sinnvoll umgesetzt werden können. Auch ein gesundes Maß an Pragmatismus schadet hierbei nicht.

Sinnvollerweise beginnt man diesen Prozess aus der Vogelperspektive, statt mit der Umsetzung einzelner, gut gemeinter Maßnahmen. Es ist sicherlich nicht falsch, eine Firewall anzuschaffen, ein Antivirus-System zu betreiben und Unternehmensdaten mit einer Backup-Software zu sichern – im Gegenteil, es gibt vermutlich kein Unternehmen, dass sich um diese Dinge nicht gekümmert haben sollte. Gesteuerte Cybersicherheit beginnt allerdings an anderer Stelle.

### **Cybersicherheit ist Chefsache!**

Vor allem sollte Cybersicherheit nicht rein aus der IT-Abteilung gesteuert werden. Die Unternehmensleitung muss den Grundstein für ein Managementsystem legen, welches mit Prozessen, Dokumentationen und Richtlinien dafür sorgt, dass der Schutzbedarf des Unternehmens festgestellt und

daraus resultierend sinnvolle Maßnahmen getroffen werden. Dabei ist wichtig zu beachten, ob es Anforderungen aus gesetzlichen, regulatorischen oder vertraglichen Bereichen zu erfüllen gibt. Dies zu berücksichtigen und auf die Unternehmens-IT zu übersetzen, stellt den ersten Schritt zu einem Informationssicherheitsmanagementsystem (oder kurz ISMS) dar.

Viele Unternehmen kennen Managementsysteme vor allem aus dem Bereich QM und sind nicht selten sogar nach ISO 9001 zertifiziert. Im Bereich der Informationssicherheit gibt es ebenfalls Standards, an denen man den Aufbau des eigenen ISMS orientieren (oder es auf dieser Basis zertifizieren) kann: ISO 27001, BSI IT-Grundschutz oder TISAX sind einige, die immer häufiger auch im Mittelstand Erwähnung finden. Inzwischen werden viele Unternehmen sogar von Kunden, Partnern oder Zulieferern aufgefordert, ihr ISMS zertifizieren zu lassen.

Diese Entwicklung bestätigt die Prognose von Gartner, dass im Jahr 2025 Cybersicherheit eine, wenn nicht die tragende Rolle bei der Risikobewertung für Kreditvergaben und Auftragsvergabe sein wird.

Eine Kernaufgabe eines ISMS ist es, die notwendigen technischen Maßnahmen für das Unternehmen zu bestimmen. Wie viele Firewalls tatsächlich benötigt werden und wie diese konfiguriert werden müssen oder wie oft Daten wohin gesichert werden und ob diese verschlüsselt werden müssen, sind Fragen, die bei der Durchführung der einzuführenden Prozesse beantwortet werden und sicherstellen,

dass das Maß an Cybersicherheit am Ende auch wirklich zum Unternehmen passt.

#### **Nicht jedes ISMS muss zertifiziert werden!**

Wenn es im Unternehmen keine Anforderung einer Zertifizierung gibt, wird zwar möglicherweise kein ISMS nach ISO 27001 benötigt. Dennoch sollte in jedem Fall sichergestellt werden, dass Sicherheitsmaßnahmen an den Schutzbedarf der Unternehmenswerte angepasst sind.

Gerade in kleinen Unternehmen reicht es dann häufig aus, Richtlinien zu erstellen, regelmäßig Überprüfungen der IT-Sicherheit durchführen zu lassen (bspw. durch Audits oder Penetrationstests), Notfallpläne zu erstellen sowie für die Sensibilisierung der MitarbeiterInnen zu sorgen – beispielsweise durch Schulungen, e-Learning oder Phishing-Simulationen. ■

## Ansprechpartner

Frank Fengel  
Protektis GmbH  
Benzstraße 2a  
63741 Aschaffenburg  
06021 6262 15-0  
frank.fengel@protektis.de  
www.protektis.de

# Alcon

## Ganz klar sehen. Meine berufliche Zukunft.

Die CIBA VISION GmbH als Teil des Alcon Konzerns ist ein führender Anbieter für Kontaktlinsen und Kontaktlinsenpflegemittel mit Sitz in Großwallstadt bei Aschaffenburg. Das Unternehmen produziert mit innovativen Hightech-Anlagen jährlich mehrere hundert Millionen Ein-Tages-Kontaktlinsen der DAILIES™ und PRECISION1™ Familie sowie TOTAL30® und die farbigen Ein-Tages-Kontaktlinsen FreshLook™ ONE-DAY.

Unsere aktuellen Stellenangebote finden Sie auf unserer Homepage [www.de.alcon.com](http://www.de.alcon.com)



## Z! DAS ZUKUNFTSMAGAZIN IM INTERVIEW MIT REINALD KEMPF



**Reinald Kempf, Geschäftsführer der echoway GmbH**

**Die Zahlen vom BSI sind eindeutig. Cyber Crime Aktivitäten nehmen ständig zu, die Bedrohungslage ist eine große Herausforderung für Unternehmen jeder Größe und Branche. Reinald Kempf ist seit vielen Jahren als Experte für Informationssicherheit Ansprechpartner für Unternehmen in der Region. Im Gespräch mit Z! Das Zukunftsmagazin erklärt er, was sich in den letzten Jahren verändert hat und worauf IT-Administratoren achten sollten.**

**Z! In der aktuellen Ausgabe des Zukunftsmagazins ist der Schwerpunkt IT-Sicherheit. Das ist doch nichts Neues, oder?**

Natürlich war das schon immer in den Unternehmen ein wichtiger Punkt, sich um die Sicherheit der Daten und IT-Systeme zu kümmern. Doch die Rahmenbedingungen waren früher ganz andere, weswegen das Thema schon sehr heiß ist. Denken Sie an die jüngsten Medienberichte mit lahmgelegten Servern, erpressten Geldern und manipulierten Prozessen.

**Z! Was hat sich also konkret an der Ausgangslage in den letzten Jahren verändert?**

Mehr als 25 Jahre gab es eine klassische Referenzinfrastruktur mit definierten Perimetern in der IT-Sicherheit. Diese war gekennzeichnet von einem zentralen Ausgang in das Internet, geschützt durch Firewall, DMZ inkl. Proxies, Serverdiensten, Portalen usw. Die Anbindung von Außenstellen erfolgte via VPN ohne lokalen Zugang zum Internet. Es gab nur wenige mobile MitarbeiterInnen, meist reduziert

auf Vertrieb, Servicetechnik, Führungsebene. In der Regel gab es keine Cloud, bestenfalls Outsourcing oder Rechenzentrumsbetrieb z. B. von SAP im externen Rechenzentrum. Daher war auch eine Absicherung der Produktion nicht nötig. Office-IT und Operational-IT (OT) waren vielfach getrennt. Oft gab es nur eine Multifaktor- bzw. Einmalkennwort-Authentisierung für Administratoren, handverlesene MitarbeiterInnen bzw. Führungsebene oder flächendeckende, statische, schlechte Kennwörter.

**Z! Und was ist jetzt anders?**

Schauen Sie sich die Aufzählung von oben nochmal genau an. Was davon gilt heute noch für moderne IT-Architekturen? Die letzten Jahre und vor allem die Pandemie haben zu massiven Veränderung der Arbeitsweisen geführt. Da ist einiges in der IT in Bewegung, doch leider haben viele im Bereich der IT-Sicherheit der Dynamik nicht folgen können oder die neue Bedrohungslage nicht erkannt.



**Z! Welche Rolle spielt aus Ihrer Sicht der Wechsel „in die Cloud“?**

Der seit Jahren wachsende Cloud-Trend ist ein Treiber für einen radikalen Paradigmenwechsel auch für die IT-Sicherheit. Früher wurden einzelne Anwendungen (SAP, MRP, ERP, Datenbanken usw.) in „privaten“ Rechenzentren von Dienstleistern betrieben. Heute werden bei vielen Unternehmen mit einer „Cloud-First“-Strategie so schnell und viel wie möglich alle Arten von Servern (IaaS), Plattformen (PaaS) oder Diensten und Anwendungen (SaaS) außer Haus in die Public Cloud migriert. Allen voran Microsoft Azure und O365 oder AWS.

Neben datenschutzrechtlichen Herausforderungen (z. B. USA „Cloud Act“ vs. DSGVO) wird nun der eingangs beschriebene Architekturansatz massiv verändert. Unverschlüsselte (extern disponierte) Inhalte und WAN-Verbindungen (z. B. MPLS) sind hier zudem oft anzutreffen. Der Perimeter ist im Gegensatz zum früheren zentralistischen Ansatz „On Premises“ plötzlich überall: Cloud, mobile Endgeräte und Mobilität inkl. Privatnutzung, Öffnung der OT in der Produktion durch Industrie 4.0 und anderer Trends, Datenzugriff von überall auf wichtige IT-Bereiche rund um die Uhr.

**Z! Und dann kam mit Corona auch noch Home Office im großen Stil.**

Ja, genau. Anfangs, ab März 2020 ging es erst mal darum, die Belegschaft überhaupt irgendwie zu Hause „arbeitsfähig“ zu bekommen. Verständlich. Fatalerweise wurde das Sicherheitskonzept reziprok zur sich entwickelnden Bedrohungslage auf Dauer aufgeweicht oder im Klartext „die Augen zuge-drückt“ und gehofft, dass nichts passiert. Typische Probleme waren und sind: Mangelnde Bandbreite des zentralen Zugangs ins Internet (inkl. Firewall, DMZ usw.), durch den sich nun manchmal statt 10 % wie früher, 90 % der Belegschaft via VPN erst mal eingewählt und dann entweder auf Unternehmensressourcen zugegriffen hat oder via besagter FW/DMZ/Proxy Infrastruktur ins Internet ging. Dazu kommt der Mangel an Hardware-Geräten wie PCs, Laptop etc. So wurden ja teilweise völlig unkontrollierte Privatrechner für den Zugriff auf Unternehmensressourcen verwendet!

**Z! Was sind die Konsequenzen?**

Die Unternehmen sind leicht verwundbar. Die Endpoint-PCs und Netze sind oft (auch heute noch) völlig unzureichend oder gar nicht geschützt. Eine Ransomware kann so bei der nächsten Einwahl per VPN zum Einfallstor werden und einen Flächenbrand auslösen. Die IT-Administratoren haben

oftmals nur mangelhaften Überblick über das, was auf ihren Servern geschieht, da sie keine geeignete Sicherheitssoftware, beispielsweise SIEM, NDR, EDR, XDR etc. nutzen und können bei Problemen nicht rechtzeitig eingreifen.

Leider haben wir das in der Praxis alles vielfach sehen müssen und Unternehmen mit 2000 Mitarbeiter waren zwei Wochen komplett ohne IT inkl. (VoIP)-Telefonie. Da funktionierten bestenfalls noch das Handy und das Fax-Gerät!

**Z! Was sagen Sie zu Leuten, die meinen: „Wir haben doch Firewalls und überall einen Virenschanner installiert“?**

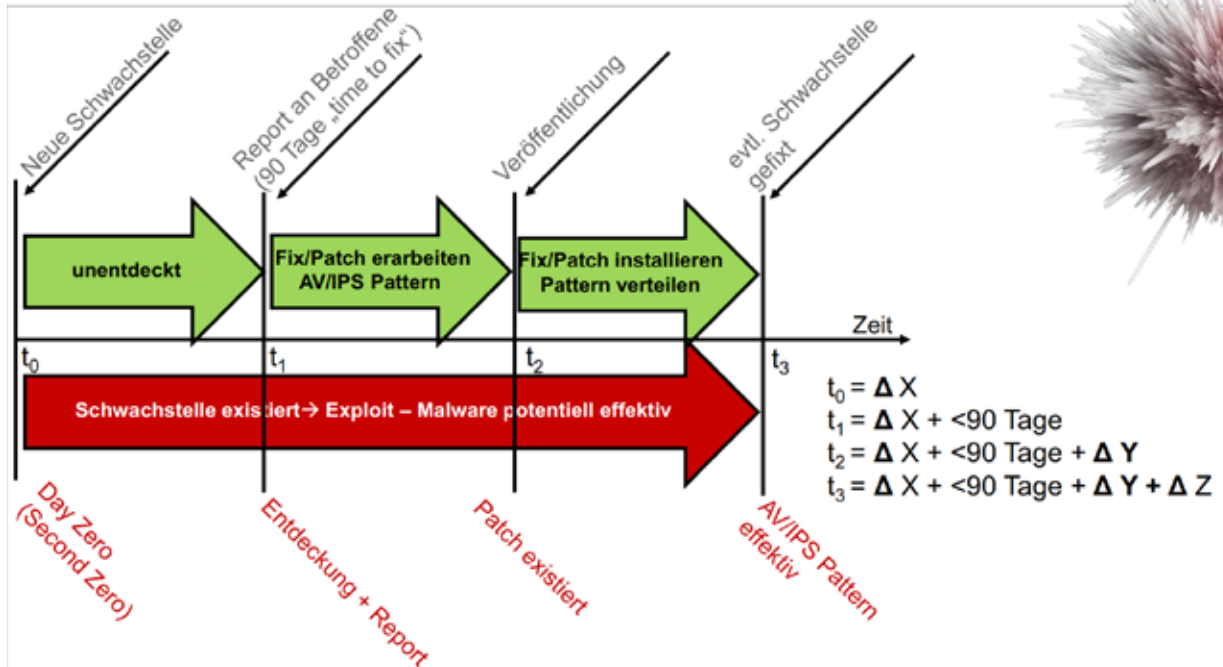
Einfache Antwort: Das reicht nicht! Mit Ransomware wie Locky wurde im Februar 2016 ein neues Zeitalter einberufen. Nein, Malware dieser Art war nichts Neues. Eindrucksvoll hat Stuxnet 2010 der Welt schon demonstriert, wie man in diesem Fall die Anreicherungsanlagen im Iran mit neuen „Cyberwaffen“ kontrolliert bzw. zerstört. Neu mit Locky ist nur die Tatsache, dass nun neben Wirtschaftsspionage und staatlich motivierten Cyberangriffen das kommerzielle Zeitalter von Malware eingeläutet wurde. Ein Milliardengeschäft mit Ransomware und erpressten Geldern. Der Trend wird erheblich zunehmen, denn im Gegensatz zu „klassischem“ Terrain wie Drogenhandel, Prostitution etc. ist man aufgrund der physischen „Abwesenheit“ im Ausland im Prinzip geschützt vor Strafverfolgung.

**Z! Politische Krisen bringen immer auch Cyber-Kriminelle auf den Plan. In Pandemiezeiten wurde von „umgeleiteten“ Fördermitteln berichtet. Was hört man zum Ukraine-Konflikt?**

Der aktuelle Ukraine-Konflikt feuert nun die bereits hinreichend bekannte, regierungsmotivierte und -gestützte Hacking-Aktivität massiv an. Parallel wird sich die kriminelle Schattenwelt, zu der auch maßgeblich russische Banden gehören, auf die neue Situation stürzen. Z. B. durch gehackte impersonifizierte Accounts oder Postfächer von Mitarbeitenden, Partnern, Kunden, Zulieferern deutscher Unternehmen. Hier scheitern dann oftmals jegliche „Awareness-Maßnahmen“ für die Mitarbeiter, wenn aus bisher vertrauenswürdigen Kommunikationsbeziehungen bzw. Quellen nun „böse“ Dateianhänge, Links oder Phishing-Mails (und Anrufe) im Tagesgeschäft einfließen. Auch in der Personalabteilung scheitert die Vorgabe „bitte nur Anhänge von E-Mails von bekannten/vertrauenswürdigen AbsenderInnen annehmen!“ BewerberInnen sind in der Regel immer unbekannt!



## Zeitlicher Verlauf Schwachstellen – Fix - Exploit



### Z! Wo liegt der Ursprung für mobile Malicious Code?

Vorläufer von Locky, Emotet & Co. gibt es grundsätzlich schon seit 25 Jahren, seit es Java und Active X auf Webseiten gibt. In den 1990er Jahren hat man erkannt, dass man durch Webdienste via Browser auch auf lokale Ressourcen auf dem PC (Registry, Dateisystem, Prozesse usw.) über z. B. eine Webseite/ein Portal zugreifen kann. Der Wegbereiter aller heutigen Web-Applikationen.

### Z! Man hört oft von Sicherheitslücken und dass diese geschlossen werden müssen.

Patchen, sprich, das Schließen von Sicherheitslücken, ist natürlich wichtig. Aber was nutzt ein Patch, wenn die Schwachstelle schon Monate (siehe Abbildung) vorher im Darknet ausgenutzt wird, bevor diese das erste Mal von einem „ethical Hacker“ oder Anwender z. B. an Microsoft, Adobe oder Apple reportet wird. Selbst dann muss es erst noch einen Patch geben und dieser muss dann noch ausgerollt und installiert sein. Das Einfallstor besteht dann über einen sehr langen Zeitraum, in welchem die besagten „alten“ Technologien absolut blind sind und keine Abwehr bieten. Es ist eben „unbekannte“ Malware. Log4j war hier Ende 2021 ein lehrhaftes, eindrückliches Beispiel. Viele Systeme dürften heute noch anfällig sein.

### Z! Welche Technologien zur Abwehr sollte jeder IT-Administrator aus Ihrer Sicht kennen?

Aus meiner Erfahrung gibt es da tatsächlich Nachholbedarf und Wissenslücken. Generell kann man die Technologien zur Malwarebekämpfung grob in zwei Klassen einteilen: Einmal die Abwehr bekannter Malware: klassische „Threat Prevention“ Anti-Spam, Antivirus, Intrusion Prevention usw. Die Technologie leistete etwa drei Jahrzehnte gute Dienste, ist aber heute bestenfalls noch für die schnelle Vorerkennung/Filterung hilfreich. Wichtiger sind also die Technologien zur Abwehr unbekannter Malware (Zero Day, Zero Second). Dazu zählen NDR, EDR, Sandboxing, CPU Level Inspection, Link Analyse und Prefetch, Content Disarm & Reconstruction bzw. Passivieren von Dokumenten. Damit werden aus z. B. aktiven E-Mail-Attachments wie PDF, XLS, DOC mit Macros bei der Erstzustellung passive Versionen ohne jegliches Gefährdungspotenzial. Natürlich kann ergänzend auch der Einsatz von Künstlicher Intelligenz helfen. Diese Dienste müsste man nun an allen oben genannten Perimetern vorschalten. Die Realität ist leider oft, dass bestenfalls der lokale Virenscanner noch den einzigen bzw. letzten Rettungsanker darstellt.

**Z! Der IT-Administrator steht vor einer Vielzahl an Produkten und Anbietern. Wie kann er sich informieren?**

Das ist in der Tat eine Herausforderung. Tatsächlich haben fast alle Anbieter solcher Sicherheitslösungen unterschiedliche Implementierungsformen und Pakete zu unterschiedlichen Kosten. Es ist aber nicht bekannt, warum diese mehr kosten und was sie dann genau mehr leisten, eben z. B. den essenziellen Schutz vor unbekannter Malware. Da ist der Markt mit vielen Schlagworten unübersichtlich, aber vor allem das Know-how auch in erfahrenen IT-Teams nicht tiefgreifend genug.

Wir bei Echoway schauen uns die Systeme unserer Kunden an und rüsten bei Bedarf nach: an der Firewall On Premises, in der Cloud (IaaS, SaaS, Container ...), auf den Endpoints, in der Mailkette, auf Servern, im Netzwerk ...

Dass dies ein lohnender Aufwand ist, zeigt z. B. die MITRE-ATT&CK Evaluation, die auf absolut neutralem Boden Virens Scanner (oder besser Endpoint-Sicherheitsprodukte) auf „Herz und Nieren“ – offen und transparent dokumentiert und gegen bekannte Herangehensweise auf Abwehrfähigkeiten unbekannter Malware prüft.<sup>1</sup>

**Z! Nochmal im Klartext, was kann man tun für die eigene IT-Sicherheit?**

Die wichtigsten Punkte sehe ich hier in der präventiven Abwehr von unbekannter Malware an allen Perimetern: On Premises, Cloud, Home Office, Produktion, Lokationen... Weiterhin die Überwachung des Netzwerkes bzw. Datenverkehrs, Echtzeitforensik, Incidence Response sowie die Konsolidierung von Lösungen, um möglichst viel Daten für intelligente (AI basierte, oder auch menschliche) Forensikanalysen und daraus abgeleitet Abwehraktivitäten in einem Guss zu haben. Auf die IT-Sicherheit zahlen sich weiterhin eine starke Authentisierung, Verschlüsselungstechnologien und die Bewusstseinsbildung der Mitarbeitenden aus.

---

<sup>1</sup> Über die MITRE-ATT&CK EVALUATION können Sie sich unter den folgenden Links informieren: <https://attack.mitre.org/matrices/enterprise/> und [https://attacker.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak\\_fin7](https://attacker.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak_fin7)

**Z! Nun passieren ja die Sachen immer bei den „Anderen“ und im eigenen Haus gibt es diese Probleme nicht.**

Guter Punkt. Aber seien Sie sich nicht zu sicher. Da läuft mehr im Verborgenen als man denkt. Es sind nicht nur die vielen sichtbaren Ransomware-Angriffe relevant, bei denen Lösegeld von Unternehmen und Organisationen gefordert werden. Der Spionage- oder Betrugstrojaner unternimmt alles, um so lange wie möglich (siehe Beispiel Stuxnet) oder für immer unentdeckt zu bleiben.

**Z! Wie kann man herausfinden, wie hoch die Bedrohungslage ist?**

Wir analysieren das gerne mit z. B. einem Zero Day Malware Audit, oft zunächst in der Mailkette, und zeigen die „Funde“ mit geeigneter Technologie, die vor dem Eingang z. B. des Exchange Servers ankommen. Die Ausgangslage ist ja die Annahme, dass durch Firewall, Threat Prevention, Proxy, E-Mail Gateway, Antispam, IPS usw. kein „böser“ Anhang, Link etc. noch ankommt. Doch siehe da: Keiner unserer (sehr sehr vielen) Audits hat in der Testphase von vier Wochen ein Ende gefunden, ohne einen gefährlichen, unbekanntes Schädling zu finden und bei eingeschaltetem Prevention Modus zu eliminieren! Der Aufwand für ein solches Testat ist i.d.R. sehr überschaubar und kein Hinderungsgrund. Das Problem betrifft alle Branchen, alle Unternehmensgrößen, sprich jeden!

**Vielen Dank, Herr Kempf für die interessanten Ausführungen und weiterhin viel Erfolg beim Kampf für mehr IT-Sicherheit.**

Das Interview führte Katja Leimeister, approdos consulting.

## Ansprechpartner

Reinald Kempf  
echoway GmbH  
Industriering 7  
63868 Großwallstadt  
06022 50872-0  
info@echoway.de  
www.echoway.de



## NEUIGKEITEN AUS DER REGION

# Transformationsprechttag für Unternehmen am Bayerischen Untermain

**Transformationsprozesse bedingt durch individualisierte Kundenanforderungen, Digitalisierung, gestiegene Ansprüche an unternehmerische Flexibilität sowie der gesellschaftliche Wunsch nach einer klimaverträglichen Wirtschaft stellen zunehmend Herausforderungen aber auch Chancen für alle Wirtschaftsbranchen dar.**

Die wirtschaftliche Transformation betrifft dabei alle Bereiche eines Unternehmens: Geschäftsmodelle und Geschäftsprozesse, Produkte und Dienstleistungen, Maschinen und Anlagen und nicht zuletzt die Belegschaft. Zur Bewältigung der damit verbundenen Herausforderungen bietet die ZENTEC GmbH Online-Orientierungsgespräche mit den Transformationslotsen und Innovationsexperten der Bayern Innovativ GmbH an. Die Berater von Bayern Innovativ stehen sowohl kleinen und mittleren als auch großen Unternehmen mit kostenfreien Innovationsimpulsen und -dienstleistungen zur Seite. In einem ersten vertraulichen 30-minütigen Online-Orientierungsgespräch werden zunächst folgende Fragen geklärt:

- Welche Unterstützungsangebote helfen Ihnen?
- Welche Kernkompetenzen bringen Sie in den Transformationsprozess ein?
- Welche Wünsche haben Sie an die bayerische Wirtschaftspolitik?

Auf Basis dieses Gesprächs erhalten Unternehmen ein auf das jeweilige Thema zugeschnittenes Angebot an kostenfreien Unterstützungsangeboten. Der nächste Transformationsprechttag findet am 13.04.2022 und am 14.04.2022 statt. Zur Terminvereinbarung steht Herr Marco Stibe telefonisch oder per E-Mail zur Verfügung. ■

### Ansprechpartner

Marco Stibe  
ZENTEC GmbH  
Kompetenznetze Bayerischer Untermain  
Industriering 7  
63868 Großwallstadt  
06022 26-1117  
stibe@zentec.de  
www.zentec.de

## Mentor und Sparringspartner: ASC unterstützt Start-up-Inkubator

**ASC Technologies AG wird Partner des Digitalen Gründerzentrums (DGZ) in Aschaffenburg. Als einer der weltweit führenden Anbieter von Software- und Cloud-Lösungen im Bereich Omni-Channel Recording, Quality Management und Analytics spielen für die ASC Technologies AG seit der Unternehmensgründung vor über 50 Jahren die Themen Zukunftsausrichtung und neue Technologien eine zentrale Rolle. Die nun geschlossene Partnerschaft mit dem lokalen Start-up-Inkubator „Digitales Gründerzentrum Alte Schlosserei“ ist daher ein logischer Schritt, junge Gründerinnen und Gründer bei ihrem Start in die Selbstständigkeit zu unterstützen.**

ASC fördert als Sparringspartner und Mentor Tech-Start-ups und bringt geschäftliche und technologische Expertise aus dem Cloud- und Software-Business ein. Das Digitale Gründerzentrum „Alte Schlosserei“ am Standort Aschaffenburg unterstützt, berät und vernetzt seit nun vier Jahren Start-ups mit hoher Innovationskraft innerhalb der Region. Damit sollen Potenziale aus dem lokalen Umkreis gefördert und genutzt werden, um den digitalen Strukturwandel zu meistern. Dank einer Förderung des Freistaats Bayern und der Unterstützung von über 20 Partnerunternehmen aus der regionalen Wirtschaft, sowie durch die Stadt Aschaffenburg und den Landkreisen Aschaffenburg und Miltenberg, können Gründerinnen und Gründer in der oft schwierigen Anfangsphase eines Start-ups umfassend unterstützt werden. Damit werden nicht nur digitale Kompetenzen, sondern auch neue Arbeitsplätze mit Zukunftsaussichten geschaffen.

### Das Fundament für die Zukunft

Künstliche Intelligenz (KI) ist ein grundlegender Bestandteil heutiger und künftiger Lösungen – nicht nur bei ASC. Das Ziel ist, effiziente selbstlernende Systeme zu entwickeln, die zur immer schnelleren und produktiveren Umsetzung von Projekten führen. „Wir möchten jungen GründerInnen und Unternehmen aktiv die Chance bieten, von unserem praktischen KI-Wissen zu profitieren. Aber nicht nur

das: Mit unserer Mitgliedschaft unterstützen wir lokale Talente als Mentoren, bei der Umsetzung ihrer neuen, digitalen und innovativen Ideen“, so Ann-Kathrin Müller, Mitglied des Aufsichtsrats bei ASC Technologies AG.

„Wir freuen uns über die Partnerschaft mit der ASC Technologies AG. Die Geschäftsbereiche des Unternehmens passen hervorragend zu unseren Start-ups. Durch die nun gestartete Zusammenarbeit haben Gründerinnen und Gründer im Mainviereck noch bessere Chancen aus ihrer Idee ein erfolgreiches Unternehmen zu entwickeln,“ sagt Florian Zashka, aktueller Interimsleiter des Digitalen Gründerzentrums „Alte Schlosserei“ in Aschaffenburg. ■

### Ansprechpartnerin

Ann-Kathrin Müller  
ASC Technologies AG  
Seibelstraße 2-4  
63768 Hösbach  
06021 5001 - 0  
AK.Mueller@asc.de  
www.asc.de

## Der neue UV-Luftreiniger Soluva Air F ist gleichzeitig leicht, leise und leistungsstark

Ein Einsatzteam in der Leitwarte, eine Besprechung vor Ort, Präsenzunterricht in der Schule mit einem Luftreiniger, den man bei seiner Arbeit fast nicht bemerkt? Genau dafür hat Heraeus Noblelight Soluva Air F entwickelt. Diese Luftreiniger mit UV-Licht sind eine Weiterentwicklung der bewährten Soluva Geräte von Heraeus Noblelight. Durch den Einsatz neuer Materialien und einer intelligenten Luftführung sind die neuen Einheiten sehr leicht und kompakt, bieten eine große Leistungsstärke und sind dabei trotzdem sehr leise.



Soluva Air F Luftreiniger mit UV-Licht arbeiten leise und dennoch leistungsstark

Die UV-Licht Experten bei Heraeus Noblelight haben Feedback von Kunden, Erfahrungen aus den eigenen Testzentren und Studienergebnisse als Grundlage für eine Weiterentwicklung genommen, das Soluva® Air F. Dieser UV-Luftreiniger ist für den Dauerbetrieb konstruiert und außergewöhnlich leise, so dass er im täglichen Betrieb kaum wahrgenommen wird. Im Gegensatz zu vergleichbaren Luftreinigungsgeräten arbeitet Soluva Air F vollständig chemiefrei, funktioniert ohne Ozon oder andere Beiprodukte und wird filterfrei betrieben, so dass keine teuren regelmäßigen Filterwechsel anfallen. Das Soluva® Air F reinigt die Raumluft mit Hilfe von UVC-Licht zuverlässig und nahezu geräuschlos von Viren, Bakterien und anderen Krankheitserregern. Mit seinem hohen Luftdurchsatz sorgt es für einen schnellen und sicheren Schutz – bei einer geprüften Virenreduktion von 99,99 %.

Das mobile und leichte Gerät ist in alle Richtungen drehbar und lässt sich einfach an der Wand anbringen oder mit einem mobilen Ständer überall im Raum aufstellen.

Heraeus Noblelight bietet Soluva® Air F, einen neu entwickelten Luftreiniger mit UV-Licht ab Februar an. Er wurde vorher intensiv getestet und eignet sich besonders für Einsatzzentralen und Leitstellen – und darüber hinaus in Kindergärten und Schulen, in Cafés und Restaurants, Wartezimmern von Arztpraxen, in Seniorenheimen, Büros oder im Einzelhandel.

### UV-Desinfektion wirkt sicher gegen Viren und deren Mutanten

Die UV-Desinfektion wirkt über eine Inaktivierung der Erbinformation, das funktioniert bei den ursprünglichen Viren ebenso wie bei neu auftauchenden Mutationen. UV-Desinfektion zerstört ebenso Grippeviren, Erkältungsviren, andere gefährliche Keime. Durch die spezielle Wirkweise der UV-Desinfektion können diese Viren auch keine Resistenzen entwickeln.

Weitere Informationen zur Luftreinigung mit UV-Licht finden Sie unter [www.Soluva.com](http://www.Soluva.com) ■

### Ansprechpartnerin

Dr. Marie-Luise Bopp  
 Heraeus Noblelight GmbH  
 Reinhard-Heraeus-Ring 7  
 63801 Kleinostheim  
 06181 35-8547  
[marie-luise.bopp@heraeus.com](mailto:marie-luise.bopp@heraeus.com)  
[www.heraeus.com](http://www.heraeus.com)

## Weiterbildung zum Betrieblichen Pflegelotsen/zur Betrieblichen Pflegelotsin findet auch 2022 wieder statt

Im Juni 2022 startet zum wiederholten Mal die Seminarreihe zum „Betrieblichen Pflegelotsen“ bzw. zur „Betrieblichen Pflegelotsin“. Das Fortbildungsangebot richtet sich an Personalverantwortliche, Betriebsräte oder andere interessierte Beschäftigte im Unternehmen, die als AnsprechpartnerInnen für das Thema Vereinbarkeit von Beruf und Pflege zur Verfügung stehen wollen. Gerade bei – häufig unerwartet – auftretenden Pflegefällen ist eine schnelle und konkrete Unterstützung wichtig. Beschäftigte, die von einem Pflegefall betroffen sind, müssen sich innerhalb kürzester Zeit neuen und belastenden Herausforderungen stellen – u.a. rechtliche und gesetzliche Rahmenbedingungen sowie Angebote und Anlaufstellen vor Ort.

Die TeilnehmerInnen erhalten in vier Vormittagsmodulen Einblicke in die rechtlichen Rahmenbedingungen, lernen die Hilfsangebote für die häusliche Pflege kennen, erfahren welche besonderen Belastungssituationen in der Pflege zu bewältigen sind und erhalten Informationen zu Angeboten und Anlaufstellen in der Region.

Betriebliche PflegelotsInnen sind Anlauf- und Beratungsstelle für Beschäftigte, die akut von einem Pflegefall

betroffen sind und sich in kürzester Zeit der neuen Herausforderung stellen müssen. Sie sind ein Beitrag des Arbeitgebers zur Familienfreundlichkeit. Anbieter der Fortbildung ist die Regionalmanagement-INITIATIVE BAYERISCHER UNTERMAIN in Kooperation mit Prädikat Mensch.

Die nächste Ausbildungsrunde am Bayerischen Untermain startet am 22. Juni 2022 in der ZENTEC. Bei Interesse wenden Sie sich an Katarina Martino. ■

### Ansprechpartnerin

Katarina Martino  
ZENTEC GmbH  
Initiative Bayerischer Untermain  
Industriering 7  
63868 Großwallstadt  
06022 26-1112  
martino@bayerischer-untermain.de  
www.bayerischer-untermain.de

## Unternehmenstransformation: C+ITEC AG wird zu Firstcom Europe AG

**Mit der Namensumbenennung ist die Transformation, die im Jahre 2016 mit dem Beitritt in die Unternehmensgruppe Firstcom Europe begann, nun nahezu abgeschlossen. Zukünftig firmiert die C+ITEC AG als Firstcom Europe AG. Damit präsentiert sich das Unternehmen nun für alle ersichtlich als europäisch agierender Telekommunikationsanbieter.**

Bereits seit längerem wird das Rebranding-Projekt vorangetrieben. So wurde bereits der Name Firstcom Europe in fast allen Geschäftsbereichen integriert. Die Außenfassade der Geschäftsräume in Goldbach weist auf den Firmensitz der Firstcom

Europe hin, zusammen mit der Marke Universe. Universe ist die eigens entwickelte und für den deutschen Markt konzipierte Cloud Telefonanlage der Firstcom Europe Unternehmensgruppe. In Zukunft hat die Firstcom Europe Gruppe speziell in

Deutschland große Ziele: „Gerade in dem Marktsegment der virtuellen Telefonie sehen wir erhebliches Marktpotenzial, das wir in den nächsten Jahren verstärkt nutzen wollen. Mit der Universe-Cloud bieten wir ein großartiges Produkt, das auch in Verbindung mit führenden Unified Communications-Anbietern betrieben werden kann. Das ist wiederum ein Türöffner für die Vermarktung über den Channel, woran wir derzeit mit großem Engagement arbeiten“, so Andreas Herget, CEO der Firstcom Europe AG.

„Durch die Umbenennung ändert sich nichts an den bisherigen Kunden-, oder Lieferantenbeziehungen und Partnerschaften. Die Firstcom Europe AG stellt, wie auch schon die C+ITEC AG, Service und Kunden an erster Stelle. Alle AnsprechpartnerInnen sind unter der gewohnten Telefonnummer erreichbar. Lediglich die Endungen der E-Mailadressen ändern sich auf @firstcomeurope.de. Die bisherigen Adressen sind allerdings noch weiter gültig. Auf bestehende Verträge oder Vereinbarungen hat der neue Name keine Auswirkung“, versichert Marko Brandt, CFO der Firstcom Europe AG.

Der Schwerpunkt von Firstcom Europe liegt weiterhin auf einer partnerschaftlichen Zusammenarbeit mit Kunden und Geschäftspartnern sowie auf

maßgeschneiderten Lösungen rund um die Kommunikationssysteme. Firstcom Europe bietet moderne Konzepte für die heutige Arbeitswelt an. In einer Arbeitswelt, in der Kunden nach Werkzeugen suchen, die ihnen die Flexibilität geben, individuell zu entscheiden, wo sie arbeiten – zuhause, unterwegs oder im Büro – und ihnen überall den Komfort von integrierten Video- Sprach- Chat- und Faxfunktionen bieten. Parallel werden Online-Plattformen aufgebaut zum selbst konfigurieren der Universe-Cloud. So sieht sich die Firstcom Europe für die Zukunft gut aufgestellt. ■

## Ansprechpartnerin

Astrid Schlosser  
Firstcom Europe AG  
Dammer Weg 51  
63773 Goldbach  
06021 4436-0  
astrid.schlosser@firstcomeurope.de  
www.firstcomeurope.de

## Beginn des neuen Förderprojekts „Weiterbildungsverbund (Automotive) Bayerischer Untermain“

Zum 01. April 2022 startet das neue Förderprojekt „Initiative Weiterbildungsverbund (Automotive) Bayerischer Untermain. Regionale Arbeitsmarkt- und Weiterbildungsakteure sowie VertreterInnen der freien Wirtschaft haben sich dazu entschlossen, das Verbundprojekt "Initiative Weiterbildungsverbund (Automotive) am Bayerischen Untermain", unter der Projektleitung der ZENTEC GmbH aktiv zu begleiten.

Ziele des Projekts sind neben der Schaffung eines aktiven länderübergreifenden Unternehmensnetzwerks die Unterstützung eines strukturierten und systematischen Aufbaus der Personalentwicklung und die Erhöhung der Beteiligung an Weiterbildungsmaßnahmen. Zum Start des Projekts werden im Rahmen einer umfassenden Bestandsaufnahme die konkreten Weiterbildungsbedarfe der Unternehmen im Bereich Automotive identifiziert. Daraus entstehen eine Reihe neuer und innovativer

Angebote für regionale Unternehmen aus der Fahrzeugindustrie. Ausführliche Informationen zum Förderprojekt erhalten Sie in der nächsten Z! Ausgabe. Für Auskünfte vorab wenden Sie sich gerne an Tobias Zenglein. ■

## Ansprechpartner

Tobias Zenglein  
ZENTEC GmbH  
Industriering 7  
63868 Großwallstadt  
Tel.: 06022 26-1008  
zenglein@zentec.de  
www.zentec.de

## Arbeitnehmer und Arbeitgeber voranbringen: Das Projekt „Weiterbildungsinitiatorin“ am Bayerischen Untermain geht weiter bis Ende 2024!

Wie können Unternehmen ihre MitarbeiterInnen für die Herausforderungen der digitalen Arbeitswelt qualifizieren? Bei dieser Frage unterstützt die Weiterbildungsinitiatorin Susanne Trunk von der SQG Strukturwandel und Qualifizierung gemeinnützige GmbH in Aschaffenburg alle interessierten ArbeitgeberInnen und ArbeitnehmerInnen in Stadt und Landkreis Aschaffenburg sowie Landkreis Miltenberg.



Susanne Trunk, Weiterbildungsinitiatorin am Bayerischen Untermain

Ende 2019 wurde Susanne Trunk vom Bayerischen Staatsministerium für Familie, Arbeit und Soziales als "Weiterbildungsinitiatorin für die Region Aschaffenburg und Miltenberg" beauftragt, in dieser Funktion Betriebe, aber auch deren MitarbeiterInnen in allen Fragen der beruflichen Weiterbildung zu beraten und den digitalen Strukturwandel in der Region Bayerischer Untermain zu begleiten. Jetzt

wurde die Beratungsstelle für berufliche Weiterbildung bis Ende 2024 verlängert.

In allen bayerischen Regierungsbezirken stehen WeiterbildungsinitiatorInnen für die Beratung in Sachen Weiterbildung bereit. Gefördert wird diese Projektstelle im Rahmen des "Pakts für berufliche Weiterbildung 4.0". Dabei handelt es sich um eine gemeinsame Initiative von Bayerischer Staatsregierung, den bayerischen IHKs und HWKs, der Vereinigung der Bayerischen Wirtschaft e.V., der Regionaldirektion Bayern der Bundesagentur für Arbeit und dem Deutschen Gewerkschaftsbund Bayern.

Unternehmen benötigen kompetente MitarbeiterInnen, um die aktuellen und künftigen technischen, wirtschaftlichen, demografischen und sozialen Herausforderungen besser bewältigen zu können. Und Beschäftigte brauchen fachliche, methodische und soziale Kompetenzen, um ihre Beschäftigungsfähigkeit zu erhalten und für zukünftige Anforderungen gut gerüstet zu sein.

Susanne Trunk sieht sich in ihrer Funktion der Weiterbildungsinitiatorin als „Lotse“, denn es geht um gezielte Weiterbildung. Diese setzt Information, Beratung und mithin überhaupt einmal Sensibilisierung und Motivierung voraus. Letztlich profitieren beide Seiten, ArbeitnehmerInnen als auch ArbeitgeberInnen, von dem Angebot.

Die Arbeit der Weiterbildungsinitiatoren beschreibt Susanne Trunk so: „Wir beraten sowohl Unternehmen als auch Beschäftigte und Arbeitnehmervertretungen rund um das Themenfeld der beruflichen Weiterbildung. Dazu entwickeln wir mit den Beschäftigten persönliche Weiterbildungsziele und unterstützen bei der Suche nach passenden Bildungsangeboten. Wir beraten neutral, unabhängig und kostenfrei. Es geht nicht darum, Kurse eines



speziellen Anbieters zu bewerben, sondern das passgenaue Weiterbildungsangebot zu identifizieren und über vorhandene Fördermöglichkeiten zu informieren.“

Weitere Informationen und Erfolgsgeschichten im Internet auf Bayerns zentralem Weiterbildungsportal [www.kommweiter.bayern.de](http://www.kommweiter.bayern.de) ■

## Ansprechpartnerin

Susanne Trunk  
SQG Strukturwandel und Qualifizierung gGmbH  
Wermbachstr. 19  
63739 Aschaffenburg  
06021 38651-12  
[susanne.trunk@sqq-aschaffenburg.de](mailto:susanne.trunk@sqq-aschaffenburg.de)  
[www.sqq-aschaffenburg.de](http://www.sqq-aschaffenburg.de)

### Über die SQG:

Die SQG gGmbH wurde 1998 als gemeinnützige Gesellschaft gegründet. Zweck der Gesellschaft ist, in Kooperation mit Unternehmen, der Agentur für Arbeit, Arbeitgeber- und Arbeitnehmerorganisationen sowie den Bildungsträgern Beratungs- und Qualifizierungsmöglichkeiten für ArbeitnehmerInnen zu realisieren, die in Folge des Strukturwandels am Bayerischen Untermain von Arbeitslosigkeit bedroht oder betroffen sind. Vorrangig als qualifizierte Transfergesellschaft und Outplacementgesellschaft.

Darüber hinaus berät und unterstützt die SQG Unternehmen, deren Interessenvertretungen und Beschäftigte bei der individuellen Gestaltung von Qualifizierungskonzepten, um den zukünftigen beruflichen Anforderungen des Arbeitsmarktes und durch digitale Transformation gerecht zu werden.

Gesellschafter und in den Gremien vertreten sind neben der Stadt Aschaffenburg die Landkreise Aschaffenburg und Miltenberg, die Agentur für Arbeit, Arbeitnehmer- und Arbeitgeberverbände, Politiker und einzelne Unternehmen der Region.

## Theo Klein + Partner feiert 30-jähriges Firmenjubiläum

**Personalberatung mit Begeisterung, Empathie und Disziplin**

**Theo Klein ist der Gründer der Theo Klein + Partner Unternehmensberatung GbR (kurz TKP) mit Sitz in Großwallstadt. Das Unternehmen wird in diesem Jahr 30 Jahre alt und ist als Personalberatung auf die Besetzung von Einkaufs- und Vertriebspositionen spezialisiert.**

### Vom Wandel in der Personalberatung

Mit Anbruch des Internetzeitalters und der Nutzung von immer mehr Sozialen Medien hat sich in der Ansprache von BewerberInnen vieles gewandelt. Waren in den 90igern noch mehrere hundert Stellenanzeigen in jeder FAZ-Ausgabe, sind heute Jobbörsen und vor allem die Sozialen Medien der „Umschlagplatz“ für Top-KandidatInnen. Damit hat sich auch das Verhalten der KandidatInnen geändert:

Waren sie früher eher der aktive Part bei der Vermittlung, indem sie sich auf die Stellenanzeigen in FAZ & Co. telefonisch gemeldet haben, gehen heute verstärkt Recruiter direkt auf latent Wechselwillige zu.

Der Qualitätsanspruch der Klienten an die KandidatInnen und den Bewerbungsprozess ist dagegen geblieben. „Wer eine Personalberatung einschaltet, erwartet die bestmöglichen derzeit verfügbaren



KandidatInnen. Die Suchmandate sind aber auch herausfordernder geworden, da der Fachkräftemangel weiter gestiegen und die Umzugsbereitschaft – selbst bei lukrativen Führungsaufgaben – immer weniger gegeben ist“, erläutert Theo Klein.

#### Heutige Herausforderungen

Die Unternehmen sehen sich in vielen Fachbereichen einem enormen Fachkräftemangel gegenüber. Geeignete KandidatInnen werden häufig über die einschlägigen Kanäle angesprochen, oft auch wenig individuell in Massenmailings. Diese Ansprache wird vielfach als nervig empfunden. Hier geht man bei Theo Klein + Partner einen anderen Weg: „Es ist wichtig, dass man den KandidatInnen zunächst gut zuhört, ihre beruflichen Wünsche und Ziele erfragt. Und erst, wenn man das Gefühl hat, dass die Person auch wirklich zur Ausschreibung passt, bringen wir das Angebot ins Spiel“, erklärt Theo Klein seine Vorgehensweise.

#### Spezialisierung von Vorteil

Bei Theo Klein + Partner kristallisiert sich in den letzten Jahren eine Spezialisierung auf Positionen im Einkauf, Vertrieb und Finanzen heraus. Damit ist das Vermittler-Team in der Lage, thematisch mitzu-

reden und kennt das jeweilige Wording. So entsteht Vertrauen auf beiden Seiten, sowohl bei den KandidatInnen als auch bei den Klienten und die Qualität und Passgenauigkeit der vorgeschlagenen BewerberInnen wird gesteigert.

#### Fachkräfte für den Mittelstand

Theo Klein + Partner haben Mandate aus Konzernen, aber auch aus weniger bekannten Unternehmen, sogenannten Hidden Champions aus dem Mittelstand, die sich mit der Ansprache geeigneter KandidatInnen aufgrund ihres geringen Bekanntheitsgrads eher schwertun. Ihnen rät der erfahrene Personalberater schneller zu werden, die BewerberInnen wertzuschätzen und das Gefühl zu vermitteln, dass man wahres Interesse an den KandidatInnen habe. Ergänzend sind wirksame Maßnahmen zur Steigerung des Bekanntheitsgrads und zum Finden und Binden der Belegschaft unerlässlich. Es braucht neben einem professionellen Recruiting also auch eine Strategie für erfolgreiches Employer Branding und Onboarding.

Mehr erfahren Sie unter [www.tklein-partner.de](http://www.tklein-partner.de). Im dort abrufbaren Interview mit Theo Klein lesen Sie von den unternehmerischen Anfängen, Trends im Recruiting-Markt und welche Herausforderungen der Mittelstand bei der Besetzung von TOP-Positionen meistern muss.

## Ansprechpartner

Theo Klein  
Theo Klein + Partner Unternehmensberatung  
Industriering 7  
63868 Großwallstadt  
06022 7090-200  
[hr@tklein-partner.de](mailto:hr@tklein-partner.de)  
[www.tklein-partner.de](http://www.tklein-partner.de)

## Theo Klein + Partner Unternehmensberatung GbR

Gründungsdatum: 1992  
Schwerpunkte: Personalberatung für Einkauf, Vertrieb, Finanzen  
Philosophie: Mit Begeisterung, Empathie und Disziplin für den Erfolg des Kunden  
Struktur: 3 Partner, 6 MitarbeiterInnen  
Standorte: Großwallstadt, Mannheim, Kiel



## STIMMEN AUS DER POLITIK

# Cyberangriffe auf die öffentliche Verwaltung – welche Gefahr besteht für bayerische Kommunen?

Server sind nicht mehr erreichbar, E-Mails können nicht versendet werden. Die Verwaltung ist lahmgelegt. Dann kommt eine Lösegeldforderung. Wenn nicht gezahlt wird, wird damit gedroht, Daten zu verschlüsseln und diese zu veröffentlichen. Ein Alptraum, nicht nur für jedes Unternehmen, sondern auch in der öffentlichen Verwaltung.

Im Juni vergangenen Jahres wurde das Verwaltungsnetz des Landkreises Anhalt-Bitterfeld Opfer eines solchen Cyberangriffs. Das IT-System des Landkreises wurde mit Schadsoftware (Ransomware) infiziert und schließlich wurden Daten verschlüsselt und abgezogen. Teile der Daten, zum Teil hochsensiblen Inhalts (Adressen, nicht-öffentliche Sitzungsprotokolle, Bankverbindungen), wurden später im Darknet veröffentlicht. Über Wochen war die Verwaltung des Landkreises nicht arbeitsfähig. Transferleistungen, z. B. Sozialhilfe konnten nicht ausgezahlt werden. Dieser IT-Sicherheitsvorfall führte zur Ausrufung des ersten Cyber-Katastrophenfalls in der Geschichte der Bundesrepublik. Die Wiederaufbauarbeiten der IT-Infrastruktur dauern vermutlich bis Mai 2022 an und werden ca. 2 Millionen Euro kosten.

Dieses Beispiel zeigt, wie verwundbar die kommunale IT-Infrastruktur ist. Nur wenige Kommunen können die Ressourcen aufbringen, um sich wirksam vor Cyberattacken zu schützen. Das ist erschreckend, wenn man bedenkt, dass das Geschäft der Cyberkri-



minalität floriert. Allein von Juni 2020 bis Mai 2021 hat die Anzahl neuer Schadprogramm-Varianten nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) um circa 144 Millionen zugenommen. ▶

Das Onlinezugangsgesetz verpflichtet Bund, Land und Kommunen, ihre Verwaltungsdienstleistungen bis Ende 2022 digital zur Verfügung zu stellen. Das erhöht die Abhängigkeit der Verwaltungsdienstleistungen von der IT und es macht die kommunale Verwaltung zu einem beliebten Angriffsobjekt für Cyberattacken. Vor diesem Hintergrund stellt sich die Frage, inwieweit bayerische Kommunen gerüstet sind, mit solchen Cyberattacken umzugehen.

Laut Auskunft der Staatsregierung auf eine Anfrage der FDP (Drs. 18/12316) liegt die IT-Sicherheit in Eigenverantwortung der Kommunen. Die Bedrohungslage wird als hoch eingestuft, denn selbst kleine Kommunen sind ohne funktionierende IT nicht arbeitsfähig.

Das Landesamt für Sicherheit und Informationstechnik (LSI) stellt hierfür seine Dienste als beratende Behörde z. B. in Bezug auf den Schutz der IT-Infrastruktur, das Notfallmanagement sowie weiteren Themen der kommunalen Informationssicherheit zur Verfügung. Darüber hinaus vergibt es das Siegel „Kommunale IT-Sicherheit“ auf Basis einer Selbstauskunft der Kommunen für eine Mindestabsicherung in der Informationssicherheit. Derzeit haben laut einer Anfrage der FDP an die Staatsregierung gerade mal 9,2 % der bayerischen Kommunen das Siegel Kommunale IT-Sicherheit erhalten (Stand: Feb. 2021, Drs. 18/19301). Zudem gibt es keine Meldepflicht der kommunalen Ebene, wie IT-Sicherheit in der Kommune umgesetzt wird. Die Staatsregierung hat also keinen Überblick darüber, wie es um die kommunale IT-Sicherheit im Freistaat tatsächlich bestellt ist. Stattdessen setzt man auf freiwilliges Engagement der Kommunen zum Besuch von Schulungen, Informationsveranstaltungen und bei Selbstauskünften. Etwaige Sanktionen bei einer Nichtumsetzung des gesetzlich geforderten Informationssicherheitskonzepts sind nicht vorgesehen.

Die Staatsregierung selbst warnt vor einer Zunahme von Cyberattacken durch zunehmende Kommerzialisierung im Bereich der Malware. Dennoch behandelt der Freistaat Bayern das Thema IT-Sicherheit weiterhin stiefmütterlich und lässt die Kommunen damit allein. Dabei zeigt doch das Beispiel aus Sachsen-Anhalt, welche Gefahr für das öffentliche Leben von einer Cyberattacke ausgeht. Vor allem kleine Gemeinden sind in Gefahr. So kennen sich hier nur wenige mit den Gefahren des Internets aus. Eine Benennung eines IT-Sicherheitsbeauftragten auf dem Papier schützt noch keine Kommune, wenn dieser nicht über entsprechenden fachlichen Hinter-

grund verfügt. Und wenn mir ein Bürgermeister als Beitrag zur Sicherheit in seiner Kommune seine Anweisung nennt, dass jede/r MitarbeiterIn nur seine eigene User-Kennzeichnung verwenden darf, ist das ein sprechendes Beispiel dafür.

Viele Kommunen unterschätzen systematisch die Gefahr eines Cyberangriffs und verlassen sich zu sehr auf bestehende Systeme. Sie sind nicht sensibilisiert für das Thema. Es braucht daher weitergehende Maßnahmen.

Die IT-Sicherheit ist die Achillesferse des Informationszeitalters. Ihre Gewährleistung ist eine Kernherausforderung der Digitalisierung, der die Staatsregierung nicht ausreichend Beachtung schenkt. Das LSI ist hervorragend aufgestellt, aber es braucht eine tatsächlich umsetzbare und agile Cybersicherheitsstrategie. Bestandteile davon müssen ein wirksames Schwachstellenmanagement und ein Recht auf Verschlüsselung sein. Die vorhandenen Kompetenzen auf Ebene des Freistaates müssen gestärkt und ausgebaut werden. Know-how in Sachen IT-Sicherheit muss für alle Gemeinden, egal welcher Größe, verfügbar sein. Dabei muss geprüft werden, welche Aspekte der IT-Sicherheit in welcher Form sinnvollerweise zentral angesiedelt werden können – mit eindeutiger Kompetenzabgrenzung, ohne Doppelstrukturen. Es braucht dringend klare Zuständigkeiten und ein starkes Engagement des Freistaates. Kommunen sollen in die Lage versetzt werden, die Gefahren für ihre Verwaltung selbst zu identifizieren und entsprechend zu beheben. Dafür braucht es eine Sensibilisierungskampagne zum Thema Cybersicherheit, sonst kann sich der Fall Anhalt-Bitterfeld auch in Bayern wiederholen.

## Ansprechpartner

Dr. Helmut Kaltenhauser MdL  
Abgeordnetenbüro  
Roßmarkt 22  
63739 Aschaffenburg  
06021 583 22 99  
helmut.kaltenhauser@fdpltby.de  
www.helmut-kaltenhauser.de

## Bayern stärkt die Cybersecurity

Zehn Stunden am Tag verbringt jeder Mensch in Deutschland durchschnittlich am Bildschirm. Das ist das Ergebnis einer repräsentativen Umfrage des Digitalverbands Bitkom vom Januar 2022. Seit dem Beginn der Corona-Pandemie ist die durchschnittliche Zeit vor dem Bildschirm pro Person damit noch einmal um zwei Stunden gestiegen. Dabei wurden die Zeiten mit dem Smartphone und die Stunden vor einem Computer-Monitor oder dem Fernseher zusammengerechnet.



So erfreulich es ist, dass viele Menschen im Home-Office arbeiten oder online einkaufen können, so besorgniserregend ist es, dass Straftäter den digitalen Raum immer stärker nutzen. 2020 stieg in Bayern die Zahl der Fälle, bei denen das Internet als Tatmittel genutzt wurde, um 20 % auf fast 36.000 Delikte. Darunter fallen vor allem Betrugshandlungen und Straftaten gegen die sexuelle Selbstbestimmung.

### Bayern baut die Bekämpfung der Cyberkriminalität bei der Polizei weiter aus

Die Bekämpfung der Cyberkriminalität wird deshalb in den kommenden Jahren eine der größten Herausforderungen für die Innere Sicherheit werden. Deshalb baut Bayern die Bekämpfung der Cyberkriminalität weiter konsequent aus.

Bei der Bayerischen Polizei sind mittlerweile rund 400 Spezialisten im Kampf gegen Kriminelle im Netz im Einsatz, die besonders aus- und fortgebildet sind:

- Darunter sind 185 IT-Kriminalisten, die nach einem Studium im Bereich der Informatik zu vollwertigen Polizeivollzugsbeamten ausgebildet wurden.
- Rund 15 weitere IT-Kriminalisten werden 2022 ihre Polizeiausbildung beenden.
- Darüber hinaus können bayernweit „Quick-Response-Teams“ rund um die Uhr alarmiert werden. Die spezialisierten IT-Ermittler und IT-forensischen Spurensicherer werden z. B. bei schwerwiegenden Cyberangriffen direkt vor Ort eingesetzt.

### Zentralstelle Cybercrime Bayern

Die Zentralstelle Cybercrime Bayern (ZCB), angesiedelt bei der Generalstaatsanwaltschaft Bamberg, ist bayernweit zuständig für die Bearbeitung herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität. Allein im Jahr 2020 leitete die ZCB fast 11.000 Ermittlungsverfahren ein.

- Technisch und ermittlungstaktisch geschulte Spezialstaatsanwälte sowie IT-Forensiker ermitteln bei Angriffen auf bedeutende Wirtschaftszweige oder bei Verfahren aus dem Bereich der organisierten Cyberkriminalität.
- Auch dann, wenn bei Verfahren der Allgemeinkriminalität ein hoher Ermittlungsaufwand im Bereich der Computer- und Informationstechnik abuarbeiten ist, werden die Staatsanwälte der Zentralstelle tätig.
- Seit August 2018 ist die ZCB zudem für herausgehobene Fälle der Wirtschaftscyberkriminalität zuständig. Die Fälle reichen von Hackerangriffen über Fälle des Vorkasse-Betrugs im Internet, z. B. durch Fake-Shops, Betrug Cybertrading-Plattformen, Fällen von Ransomware bis hin zum Handel mit Waffen, Drogen, Falschgeld und Kinderpornographie im Darknet.

### **Bekämpfung von Kinderpornographie und sexuellem Missbrauch im Internet**

Um die Ermittlungsstrukturen zu optimieren und den Verfolgungsdruck auf die Täter weiter zu erhöhen, wurde im Oktober 2020 bei der ZCB das Zentrum zur Bekämpfung von Kinderpornographie und sexuellem Missbrauch im Internet (ZKI) gegründet:

- Ein Team von Spezialstaatsanwälten sowie IT-Spezialisten ermittelt wegen Kinderpornographie und sexuellem Missbrauch im Internet.
- Im Fokus ist die Verfolgung von Betreibern und Nutzern von Darknet-Foren, die kinderpornographisches Material herstellen, posten oder damit handeln.

### **Cybersecurity ist der Schlüssel für eine erfolgreiche digitale Transformation**

Um Unternehmen (dabei vor allem KMU) aller Branchen, Forschungseinrichtungen und die öffentliche Hand zu unterstützen, hat Bayern Innovativ eine eigene Themenplattform Cybersecurity eingerichtet. Sie vernetzt Initiativen in Bayern, Deutschland sowie mit internationalen Partnerländern, um folgende Ziele zu erreichen.

- Stärkung der Wettbewerbsfähigkeit bayerischer Unternehmen
- Erhöhung der Resilienz bayerischer Unternehmen (v.a. KMU) gegen Cyber-Angriffe

- Erhöhung des Bewusstseins für Cybersecurity in Wirtschaft und Gesellschaft
- Unterstützung des öffentlichen Diskurses zum Thema Cybersecurity

Zu den Partnern der Themenplattform zählen Initiativen wie der Bayerische IT-Sicherheitscluster in Regensburg sowie die bayerischen IHKs und der vbw, aber auch internationale Netzwerke zum Thema IT-Security. Alle Informationen dazu unter:

[www.bayern-innovativ.de/netzwerke-und-thinknet/uebersicht-digitalisierung/cybersecurity](http://www.bayern-innovativ.de/netzwerke-und-thinknet/uebersicht-digitalisierung/cybersecurity)

## Ansprechpartner

Berthold Rüth, MdL  
Abgeordnetenbüro  
Bayernstr. 46  
63863 Eschau  
09374 970026  
[berthold.rueth@csu-landtag.de](mailto:berthold.rueth@csu-landtag.de)  
[www.berthold-rueth.de](http://www.berthold-rueth.de)



Digitalisierung und Vernetzung bringen viele Vorteile und Erleichterungen – auch für den Kontakt mit Verwaltungen. Jedoch mit der Zunahme an wertvollen Daten erkennen wir auch die Vulnerabilität vernetzter Systeme. Cybercrime hat sich zu einem Geschäftsmodell entwickelt. Wer kennt sie nicht, die Drohungen per E-Mail, dass ein Fremder Zugriff auf die eigenen Daten, Fotos und Dokumente hat und diese veröffentlichen oder verschlüsseln wird, sofern nicht binnen kurzer Zeit Summe X in Kryptowährung gezahlt wird. Nun ist an solchen Warnungen häufig nicht viel dran, die tatsächlichen Cybercrime-Angriffe werden aber immer ausgefeilter und verursachen in Unternehmen, Verwaltungen und sonstigen Organisationen, gleich welcher Größe oder Branche, große Schäden. Schnell werden diese existenzbedrohend, wenn betriebliche Prozesse unterbrochen werden, Termine nicht mehr gehalten werden oder finanzielle Einbußen drohen. Aktuell wird uns deutlich vor Augen geführt, dass

auch Staaten systematisch die IT-Sicherheit anderer Staaten oder Unternehmen angreifen und vor wirtschaftskriminellen Handlungen nicht halt machen, um den betroffenen Organisationen Schaden zuzufügen oder Wettbewerbsvorteile zu erlangen.

Dem präventiven Schutz der Informations- und Kommunikationssysteme gegen Angriffe von außen kommt demnach eine hohe Bedeutung zu. Für unsere Verwaltungen, als auch für die Unternehmen in der Region ist dies eine große und mitunter kostenintensive Herausforderung. Gleichwohl sehen wir an der aktuellen Ausgabe von Z! Das Zukunftsmagazin, dass in der Region zahlreiche Unternehmen und FachexpertInnen im Markt aktiv sind und die notwendige Unterstützung bei der Sicherung sensibler IT-Infrastrukturen geben können. Hier besteht sicherlich auch ein Zukunftsmarkt für AbsolventInnen der Technischen Hochschule, Ausbildungsberufe und innovative Gründungsideen. Als Region geben wir alles, um sowohl für die Unternehmen als auch für den Branchennachwuchs optimale Rahmenbedingungen zu schaffen, indem wir zur Vernetzung beitragen und eine Vielzahl von Beratungsangeboten für Gründung, Innovation und Förderbedarfe anbieten.

Ihr  
Jens Marco Scherf

### Ansprechpartnerin

Susanne Seidel  
Landratsamt Miltenberg  
Brückenstr. 2  
63897 Miltenberg  
landrat@lra-mil.de  
www.landratsamt-miltenberg.de



Mit freundlicher Unterstützung von

