Dipl.-Ing. Thomas Käfer, M.Sc.
Öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung
Master of Science Digitale Forensik
Elchenrather Weide 20 - 52146 Würselen
Tel. 02405/47949-0 - Mobil 0172/2403674
https://www.KaeferLive.de - E-Mail: Kaefer@KaeferLive.de

Dipl.-Ing. M.Sc.
Thomas Käfer
EDV Sachverständiger

**Success Story ISO 27001**

**Abstract – Worum geht es?**
*Im nachfolgenden Artikel geht es um den Weg zu einer ISO 27001 Zertifizierung, was ein ISMS ist und warum man beides nicht nur als IT-Unternehmen haben sollte. Der zugegeben nicht ganz unaufwändige Prozess ist ein wichtiger Baustein zu mehr IT-Sicherheit und vielleicht der entscheidende Punkt, warum das eigene Unternehmen nicht gehackt wird oder die Auswirkungen zumindest nicht so schlimm ausfallen.*

Spätestens seit 2022 gehört es schon zum guten Ton, „gehackt“ zu werden. Die Nachrichten sind im Monatstakt voll von neuen Meldungen über spektakuläre Angriffe auf die IT großer Unternehmen und Organisationen. Mal trifft es die gesamten IHK Deutschlands, mal große Krankenhäuser, dann wird ein ganzer Verkehrsflughafen lahmgelegt oder die gesamte öffentliche IT von rund 70 Kommunen. Allein 2023 hat es mindestens 60 Organisationen gegeben, die Opfer eines IT-Angriffs wurden und über die in der Presse berichtet wurde. Die Dunkelziffer dürfte höher liegen, denn nicht jede Firma macht einen solchen Incident öffentlich. So gibt es Abschätzungen z.B. nach einer repräsentativen Ipsos-Umfrage[1], dass 11% der befragten 501 Unternehmen ab 10 Mitarbeiter im Jahr 2023 von einem IT-Sicherheitsvorfall betroffen waren. Das entspricht etwa 50.000 Unternehmen dieser Größenklasse in der gesamten BRD. Da greift also eher der Spruch: Es ist nicht die Frage, ob man gehackt wird, sondern wann.

Das Ziel der Angreifer, die mittlerweile nicht mehr allein aus „Spaß“ und Interesse andere Systeme nach Schwachstellen untersuchen, ist hochprofessionell. Es geht immer um Geld. Um viel Geld. Meist wird eine Doppel-Erpressung versucht. Die Täter drohen zum einen damit, erbeutete Daten zu veröffentlichen bzw. im Darknet gewinnbringend weiterzuverkaufen und zum anderen legen sie mit spezieller Verschlüsselungs-Software die gesamte IT des Unternehmens (im Idealfall incl. Backup) lahm. Gegen Einwurf kleiner Münzen in Form von Bitcoins kann man sich dann den Schlüssel zum Entschlüsseln der eigenen Systeme kaufen und das Versprechen erhoffen, dass die Daten nicht verkauft werden. An Hackerehre sollte man da nicht appellieren oder darauf vertrauen, denn auch bei Zahlung des Lösegelds hat man keine Garantie, dass nicht doch ein Teil verschlüsselt bleibt oder nachher z.B. personenbezogene Daten irgendwo im Netz auftauchen. Und: Die bösen Buben sind immer noch im eigenen Netz, denn selbst wenn man mit dem erkauften Schlüssel alle Systeme wieder entschlüsseln kann, ist die Schwachstelle, über die die Angreifer ins Netz gelangt sind, noch nicht geschlossen.

[1] https://www.tuev-verband.de/pressemitteilungen/gut-jedes-zehnte-unternehmen-erfolgreich-gehackt

Schlimmer noch: Durch sogenannte Anti-Forensik-Maßnahmen verwischen gewiefte Hacker ihre Spuren und verhindern so oft erfolgreich, dass der tatsächlich genutzte Angriffsvektor im Dunklen bleibt. Der nächste Hacker wartet dann schon an der nicht richtig verschlossenen Tür und erfreut sich an einem weiterhin kompromittierten bzw. kompromittierbaren Netz und einer satten Einnahmequelle.

**Das Problem**


IT Systeme sind nie sicher, außer die Software ist trivial wie folgender Code {}. Als Betreiber muss man also versuchen, seine Systeme so sicher wie möglich zu machen und durch mehrstufige Sicherheitsvorkehrungen und Backups **immer** gegen jeden Angreifer zu gewinnen. Der Angreifer braucht hingegen nur **einmal** erfolgreich zu sein. Und das Pareto-Prinzip lehrt uns, dass man mit 20% der Kosten 80% der Leistung erzielen kann. Das bedeutet dann aber auch, dass die restlichen 20% Sicherheit 80% der Kosten verursachen. Daher bleibt dann schnell ein Gap übrig, dass man ja prima durch eine Cyber- und Betriebsausfall-Versicherung schließen kann. Die verhindert nur leider nicht, dass man gehackt wird, sondern lindert nur die Folgen – falls sie denn auch greift. Denn das Bestreben jeder Versicherung ist, möglichst viel Beiträge zu erhalten und möglichst wenig Schaden regulieren zu müssen. Da reicht dann schon vielleicht, dass man ein paar vorvertragliche Pflichten verletzt oder den Fragebogen zur Risikoeinschätzung etwas zu optimistisch und beschönigend ausgefüllt hat. Stellt ein von der Versicherung beauftragter Forensiker nämlich im Schadenfall fest, dass es Vorschäden vor Abschluss der Versicherung gab oder dass die IT grob fahrlässig nicht dem Stand der Technik (Sicherheit) entsprochen hat, dann ist die Deckungszusage in weite Ferne gerückt. Und so ein Systemausfall durch eine massive Verschlüsselungsattacke ist nicht von heute auf morgen wieder ausgebügelt.

Je nach Größe und Komplexität der IT dauert es Tage, Wochen, meist aber Monate, bis zunächst der Basisbetrieb und später die vollständige Systemverfügbarkeit wieder hergestellt ist. Und aus den Nacharbeiten zu einem massiven Security-Incident wird schnell ein Nachfolgeprojekt, welches sich über 1-2 Jahre hinziehen kann. Und es kostet wieder Geld. Das muss man dann noch haben, denn während die IT am Boden liegt, sind die meisten Unternehmen und Organisationen handlungsunfähig und verdienen kein Geld mehr. Dann stellt sich die Frage, ob sich das Unternehmen überhaupt noch von dem Angriff erholt. Das Lösegeld zu zahlen, ist auch aus einem weiteren Grund keine gute Idee. Da man es auf der anderen Seite mit organisierter Kriminalität zu tun hat, die oft auch noch staatlich geduldet oder gar unterstützt wird, kommt man so gut wie nie an die Täter heran und macht sich durch die Zahlung als Geschäftsführer / Gesellschafter ggf. sogar noch strafbar. Denn man unterstützt durch die Zahlung eine kriminelle Vereinigung oder gar eine Terrorgruppe, die das Geld für weitere Attacken einsetzen könnte.

Auch wenn das nicht final geklärt und unter Juristen offenbar gerade heiß diskutiert wird, hat man nachher nur die Wahl zwischen Pest und Cholera. Man denke an den Betreiber eines Krankenhauses: Nicht zahlen und Patienten sterben lassen, weil man sie nicht adäquat versorgen kann oder zahlen und nachher vor dem Kadi landen.

**Lösungen**

Alles irgendwie doof. Einzig bei gehackten Behörden merkt man kaum einen Unterschied zu vorher. Da läuft alles langsam, wie bisher und auch die Systemwiederherstellung geht schleppender voran als in der Industrie und bei Dienstleistern.

Und warum das Ganze? Weil IT-Sicherheit Geld kostet und ansonsten keinen Nutzen bringt. Zumindest solange oder gerade weil nichts passiert.

Und wenn IT-Systeme über Monate nicht wieder in Gang kommen, dann sehr wahrscheinlich, weil sie schlecht konzipiert sind (waren) und weil in der Krise zu wenig Geld für wirklich gute Fachleute ausgegeben wird, die das Schiff (oder den Tanker) wieder flott „flott“ machen.

So, genug der Witzeleien. Wie verhindert man das Ganze?

Bad News first: Es gibt keinen 100% Schutz und keine Garantie, dass es das eigene Unternehmen nicht trifft.

Aber man kann die Eintrittswahrscheinlichkeit und den Impact im Fall der Fälle erheblich reduzieren.

Gut ist in jedem Fall, wenn man ein oder mehrere funktionierende und nicht kompromittierte Backups aller essenziellen Systeme und Daten hat und erst gar nicht gezwungen ist, das Lösegeld zu zahlen. Diese Backups müssen unbedingt vom Zugriff der Hacker geschützt werden (z.B. durch physikalisch ausgelagerte Medien oder echten Überschreib- und Löschschutz für eine ausreichend lange Zeit), denn ansonsten ist buchstäblich alles verloren.

**Security-Baustein ISO 27001 Zertifizierung**

Jetzt kann man sich berechtigt fragen, ob ein auf der Website veröffentlichtes ISO-Zertifikat einen Angreifer abschreckt oder gar abhält, die IT anzugreifen. Sicher nicht. Er liest es wahrscheinlich nicht einmal. Aber das, was hinter der Zertifizierung steckt bzw. die Voraussetzung für den Erhalt eines solchen Zertifikats ist, wird die Hürden für einen erfolgreichen Angriff erheblich steigern. Tatsächlich gibt es offenbar noch keine Studie, die zeigt, dass ISO 27001-zertifizierte Unternehmen seltener Opfer einer Attacke wurden.
Überraschen würde so ein Ergebnis sicher nicht.

Denn Hacker sind auch nur IT-ler und die sind bekanntlich faul. Wenn der Hack bei Unternehmen „A“ nicht gelingt, weil die Hürden zu hoch sind und sich der Angreifer ständig mit Rückschlägen in seiner Arbeit abfinden muss, zieht er weiter zum nächsten potenziellen Opfer „B“ – genauso wie der handelsübliche Einbrecher von Tür zu Tür weiterzieht, bis er die einfache und lohnende Gelegenheit findet.

**Worum geht es also bei der ISO 27001?**

Die ISO 27001 ist ganz eng mit der Einführung und dem Betrieb eines **I**nformations **S**icherheits **M**anagement **S**ystems (ISMS) verknüpft. Mit einem ISMS erfasst und bewertet man alle Risiken rund um den Betrieb einer IT-Landschaft. Damit man das kann, muss man zunächst die Assets kennen, die man schützen will. Also ist im dem ISMS wiederum ein Asset-Management verknüpft, welches vom Smartphone, über das Dienst-Laptop und die On-Prem-Server bis hin zu Cloud-Diensten dafür sorgt, dass man alle Komponenten der Unternehmens-IT kennt. Denn nur was man inventarisiert hat, kann man bewerten und schützen (Vorsicht vor sogenannter Schatten-IT!).

Und dabei geht es nicht nur um Dinge, die man anfassen kann, sondern auch um Software und Dienste und natürlich um Menschen (gut, die kann man auch anfassen). Und wenn wir hier von Menschen reden, dann sind das zum einen die eigenen Mitarbeiter und zum anderen Dienstleister, die Services für das Unternehmen erbringen.

Also wird man alle Lieferanten und Dienstleister, die für ein Unternehmen tätig sind, genauso unter die Lupe nehmen, wie Hard- und Software der eigenen IT. Natürlich ist ein Kfz-Betrieb, der die Firmenwagen wartet oder der Caterer, der auf der Weihnachtsfeier für Essen und Getränke sorgt, sehr wichtig, aber solche Dienstleister haben eher keinen Impact auf die IT-Sicherheit. Aber was ist mit der Putzfrau – äh, sorry – dem Reinigungspersonal? Die haben ja auch nichts mit der IT zu tun, oder doch? Aufgepasst: Das Reinigungspersonal hat oft Generalschlüssel und kommt meist in jeden Raum – einschließlich einem Serverraum in einem kleineren Unternehmen – mindestens aber in normale Büroräume, wo der eine oder andere PC vollkommen ungeschützt herumsteht und das Passwort vielleicht unter der Tastatur oder direkt am Bildschirm klebt. Sie merken, worauf das hinausläuft?

**Was bringt eine ISO 27001-Zertifizierung?**

Zentrale Aufgabe eines ISMS ist es daher, Risiken für die IT zu identifizieren, zu bewerten und Eintrittswahrscheinlichkeit und Auswirkungen bei einer möglichen Kompromittierung oder einem Schaden durch Feuer, Wasser, Naturkatastrophen u.ä. auf ein akzeptables Maß zu senken. „Akzeptabel“ kann dabei bedeuten, dass man das nicht auszuschließende Rest-Risiko einfach hinnimmt, wenn man Eintrittswahrscheinlichkeit und Impact guten Gewissens als unwahrscheinlich und beherrschbar einstufen kann. Wozu gibt es schließlich Versicherungen und eine bisschen Risiko ist okay, oder?

Das ISMS macht aber vor allem die Aufgaben sichtbar, bei denen eine hohe Eintrittswahrscheinlichkeit für eine Schädigung besteht und/oder ein hoher Schaden entstehen kann. Sind Eintrittswahrscheinlichkeit und Schadenshöhe im roten Bereich (in der Risikomatrix im oberen rechten Quadranten), dann sind das die Punkte, denen man sich mit Priorität zuwenden muss.

Bei neu zu implementieren Systemen helfen Richtlinien den Administratoren und beauftragten Dienstleistern die Systeme nicht nur funktional „zum Fliegen zu bekommen“, sondern sie auch Security-technisch so sicher zu machen, dass sie nicht bei der ersten Gelegenheit wieder „vom Himmel geholt werden“.

Und wenn es dann zu einem Security- oder Datenschutz-Vorfall gekommen ist, hilft ein ISMS auch hier weiter. Durch festgelegte Meldeketten und Verfahren wird dazu beigetragen, dass nicht alle konzeptlos umherrennen oder sich wegducken, sondern dass zielführend der Schaden eingedämmt und minimiert wird.

Last but not least wird nach außen gezeigt, dass man es mit der IT-Sicherheit ernst meint. Das bringt ein Plus beim Abschluss einer Cyber-Versicherung, ist ggf. sogar gesetzliche Vorschrift oder wird bei öffentlichen Ausschreibungen bzw. Auftragsvergaben größerer Unternehmen einfach verlangt.

**Was kostet eine ISO 27001 Zertifizierung?**

Eine Zertifizierung ist nicht billig. Man braucht ein ISMS (incl. Einführung und Betrieb), eigene Mitarbeiter für die Umsetzung der ISO, externe Berater und vor allem einen akkreditierten Auditor (am besten von der Deutschen Akkreditierungsstelle - DAkkS). Und das Ganze ist keine Einmalinvestition. Jedes Jahr muss das Zertifikat erneuert und die Sache ohnehin gelebt werden. Da kommt also vor allem initial schnell ein hoher fünf-stelliger Betrag zusammen.

Und bitte auch die „Eh da“-Kosten nicht vergessen. Der Weg zur Erstzertifizierung und das nachfolgende aktive Leben des ISO-Gedankens kostet auch Zeit der eigenen Mannschaft, auch wenn die „eh da“ sind.

**Wie kommt man nun zur ISO 27001 Zertifizierung?**

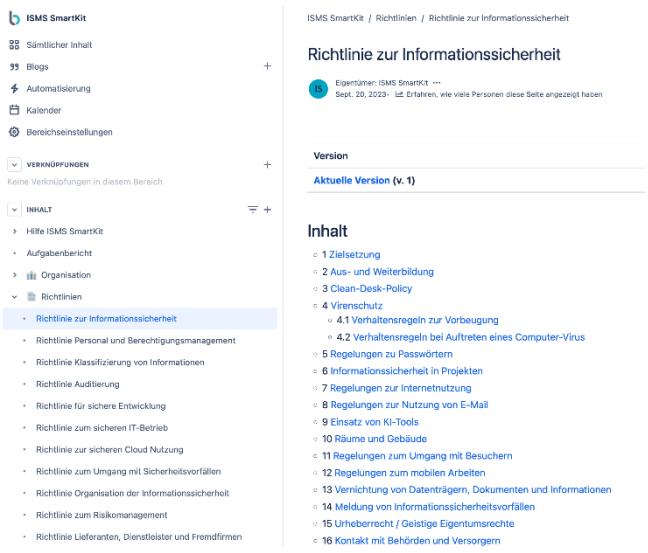
Ein ISO 27001 Zertifikat bekommt man von einer entsprechenden Zertifizierungsstelle und dort durch einen Auditor, der das Unternehmen im Rahmen von Befragungen, Begehungen und Sichten von Dokumenten und Richtlinien darauf prüft, ob alle Anforderungen (93 Maßnahmen oder Controls nach ISO 27001:2022) der Norm in einem ausreichenden Reifegrad umgesetzt sind. Am Anfang akzeptiert man einen etwas geringeren Reifegrad, erwartet aber dann bei den notwendigen Re-Zertifizierungen, dass das ISMS lebt und der Gedanke der ISO 27001 im Unternehmen auch gelebt wird. Dadurch erhöht sich in der Folge auch der Reifegrad. Keine gute Idee ist, die ISO 27001 immer nur dann zu beachten, wenn wieder mal die Zertifizierung bzw. das Audit vor der Tür stehen.

Der Auditor ist hierbei nicht Ihr Freund. Er ist ein Prüfer. Und daher wird er sein Augenmerk darauf legen, Fehler und Schwächen zu finden und erst dann ein Zertifikat ausstellen, wenn eine gewissen Hürde genommen ist.

## Welches ISMS nimmt man? Empfehlung ISMS Smartkit von Byght!

Damit Sie bzw. Ihr Unternehmen zertifizierungsfähig sind bzw. werden, brauchen Sie ein ISMS, denn streng genommen wird dieses bzw. seine Umsetzung zertifiziert. Wenn Sie noch keins haben, dann ist das ISMS Smartkit von Byght eine gute Lösung: https://byght.io/isms-smartkit/ .

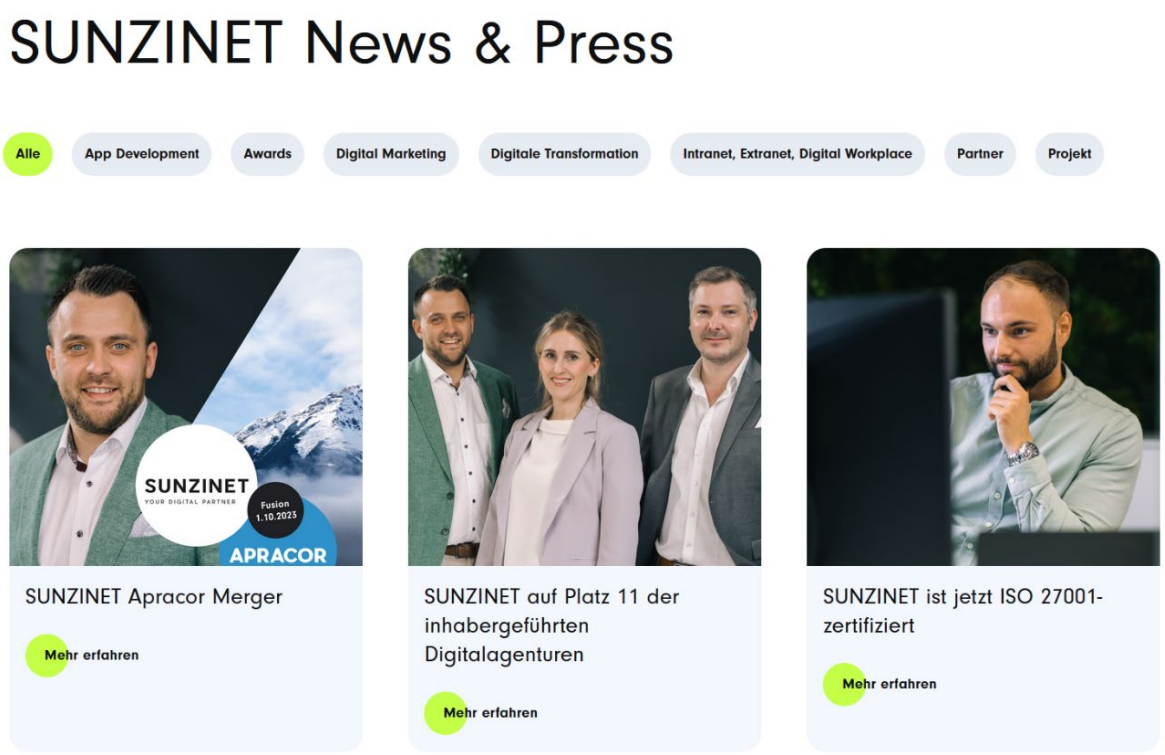

Für die Einführung des ISMS und die Befüllung der Hülle mit Leben (Richtlinien, Asset-Register, Lieferanten, Risikobetrachtungen uvm.) brauchen Sie eigene Man- und Woman-Power und man kann das komplett mit eigenen Leuten machen. Es empfiehlt sich aber, sich hier schon externe Hilfe zu holen. Mit externem Sachverstand kann man die eigenen Mitarbeiter, die die Inhalte für das ISMS liefern müssen, effektiv anleiten und führen und es steht ein Sparringspartner zur Verfügung, der ohne Betriebsblindheit und weitestgehend objektiv die Sachlage beurteilen kann. Er hilft dann, die Firma fit für das eigentliche Audit zu machen. Und er legt die Finger in Wunden, von denen Sie noch nichts wussten. Nicht, um Ihnen weh zu tun, sondern konstruktiv, um diese Schwachstellen zu schließen, bevor sie der Auditor entdeckt – oder noch schlimmer: Ein Hacker.




Und jetzt lassen wir die Katze aus dem Sack, warum ich mir die Mühe gemacht habe, rund sieben Seiten DIN A4 zum Thema zu schreiben: Dieser externe Sachverständige kann ich sein.

Kontaktieren Sie mich und wir reden weiter [Kontaktdaten siehe unten / letzte Seite]

**Referenz gefällig?**




Seit 2015 betreue ich die SUNZINET GmbH – eine der führenden Digitalagenturen Deutschlands – in Datenschutzfragen als betrieblicher Datenschutzbeauftragter. Natürlich ist Datenschutz eng mit dem noch wichtigeren Thema Datensicherheit verbunden, denn ohne Datensicherheit gibt es gar keinen Datenschutz. So war es fast eine logische Konsequenz, SUNZINET im Jahr 2023 beim nächsten Schritt, der Zertifizierung nach ISO 27001, zu begleiten. Daher habe ich Anfang 2023 auch die Rolle des CISO (Chief Information Security Officer) übernommen und die Einführung des neuen ISMS Smartkit der Firma Byght maßgeblich umgesetzt. Das Tool hat uns enorm dabei geholfen, die anstehenden Aufgaben bis hin zur Zertifizierungsfähigkeit in einem engen Zeitrahmen von nur 6 Monaten erfolgreich zu meistern. Natürlich haben wir nicht bei Null angefangen, viele Richtlinien und Arbeitsanweisungen waren bereits geschrieben und im Unternehmen etabliert. Somit haben die Vorlagen und das Gerüst zur Abbildung der ISO 27001 durch das ISMS Smartkit perfekt gepasst. Und auch der Support durch Byght war vorbildlich. Gerade in der heißen Phase der Umstellung der Norm auf die Version ISO 27001:2022 war es enorm hilfreich, die neuen Controls direkt als „Grundbetankung“ im ISMS wiederzufinden. So war es immer noch viel Arbeit, runde 50 Aufgabenblöcke mit den 93 Maßnahmen nach ISO 27001:2022 abzuarbeiten und die Texte mit Leben zu füllen, aber wir hatten einen klaren Plan vor Augen. Seither lebt das ISMS, wird aktiv genutzt, ständig erweitert und mit neuen Daten gefüttert. Selbst der noch so kleinste Sicherheitsvorfall wird im ISMS dokumentiert und anhand eines Incident Response Plans und definierten Meldeketten zügig bearbeitet. Zum Glück – oder sollen wir schon sagen: Dank ISO 27001 – gab es bisher keinen schwerwiegenden Sicherheitsvorfall. Damit das so bleibt, arbeiten wir ständig weiter an dem Thema Security – und das nicht nur, um ein Jahr später eine Re-Zertifizierung zu erhalten. SUNIZNET hat verstanden, dass IT-Sicherheit elementar ist – für das eigene Unternehmen sowie für die Kunden und deren Projekte.

## Und wenn der Incident schon eingetreten ist?


Eigentlich ist mir fast egal, wann Sie mich anrufen und in welcher Funktion ich auftrete. Aber im Ernst: Entspannter ist es, wenn ich Sie beraten kann, ohne dass es einen IT-Sicherheitsvorfall gegeben hat. Aber wenn doch, dann kann auch ein externer Krisenberater wichtige Unterstützung und Orientierung geben. Denn im Stressfall vergisst man im Rahmen des Incident Response leicht etwas und es gilt verschiedenste Institutionen und Dienstleister (Polizei, Versicherung, Forensiker, Datenschutzbehörde, externe IT Dienstleister, Juristen, Presse uvm.) und dabei auch noch die eigene IT-Mannschaft zu orchestrieren. Das ist dann ein im wahrsten Sinne des Wortes spannendes Spannungsfeld. Konkurrierende Anforderungen wie Eindämmung des Schadens, Stoppen des Angriffs, Aufklärung des Einfallvektors (incl. Schließen der ausgenutzten Lücken) stehen im Gegensatz zum Wunsch nach schneller Wiederherstellung der Daten und dem Wiederanlauf der Systeme zur Wiederverwendung der Betriebsfähigkeit.

Auch hier kann ich gerne behilflich sein. Aber wie gesagt: Lassen Sie uns lieber vorher reden. Das ist viel entspannter und preiswerter.

Dipl.-Ing. Thomas Käfer, M.Sc.

Von der IHK Aachen öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung - Master of Science Digitale Forensik

Elchenrather Weide 20 - D-52146 Würselen - Germany
Telefon: +49 (0) 2405 47949-0
E-Mail: kaefer@kaeferlive.de - Web: https://www.KaeferLive.de