11/24

securemag

Aktuelle Entwicklungen -
worauf zu achten ist
(Seite 3)

24x7 Erkennung und Abwehr
von Cyberangriffen
(Seite 6)

Das C-Level Update

Empfehlungen zur Informationssicherheit.

Einleitung

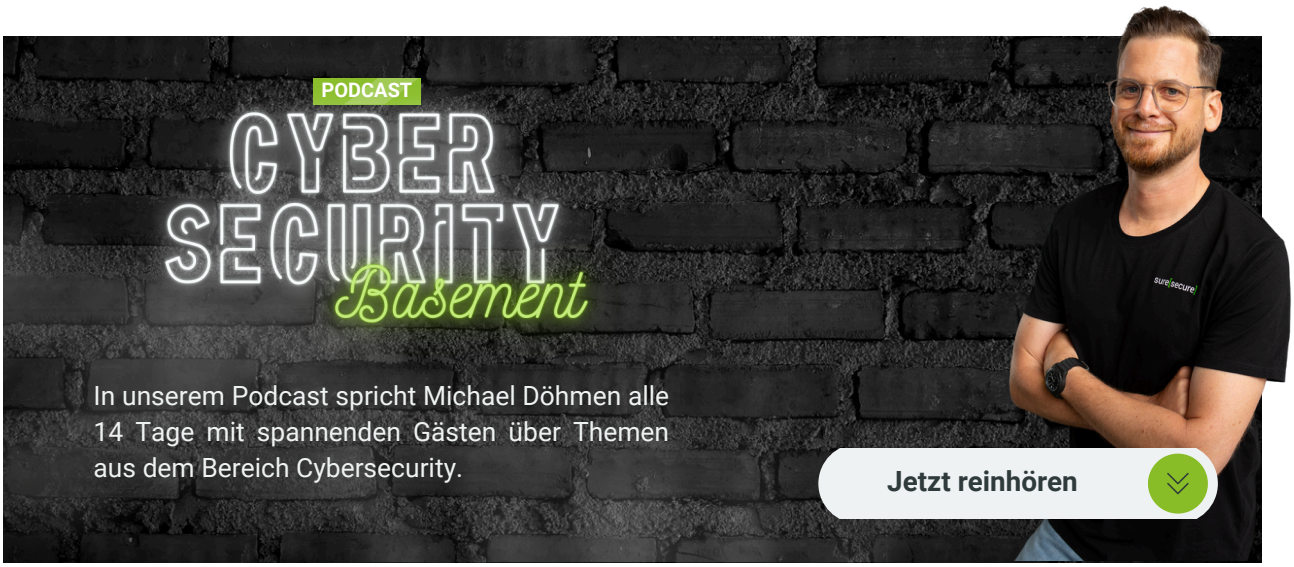
Als Geschäftsführer der suresecure GmbH bin ich dafür verantwortlich, dass unser Geschäft läuft. Aber was heißt das genau? Was bedeutet es, wenn es ***„läuft“***? Wenn es „läuft“, dann meine ich als Geschäftsführer, dass das Unternehmen profitabel wirtschaftet und das signifikantes Wachstum erkennbar ist. Denn nur wer profitabel ist, kann investieren – gerade in der heutigen Zeit, in der die Innovationszyklen immer kürzer werden.

Wer heute nicht ständig sein Geschäftsmodell weiterentwickelt und investiert, der kann morgen schon überholt werden oder sogar in der Bedeutungslosigkeit verschwinden.

Denn die digitale Transformation hält an. Auf der Suche nach Effizienz werden immer mehr Geschäftsprozesse digitalisiert und in die Cloud migriert. Das Vertrauen in die Cloud-Provider wächst und die neuen Errungenschaften von künstlichen Intelligenzen sind mit eigener Hardware kaum zu realisieren. Hier ist die Entwicklung gerade noch am Anfang.

Diese Entwicklungen machen unsere Wertschöpfung immer abhängiger von der IT- und OT-Infrastruktur. Dieser Bereich wird zur Achillesferse der Unternehmen. Wird hier fahrlässig gehandelt, kann ein erfolgreicher Cyberangriff zu enormen Schäden führen. Nicht selten werden wir bei Sicherheitsvorfällen von den Vorständen gefragt:

„Es ist doch nur unsere IT betroffen, warum funktioniert hier nichts mehr?“ Weil im schlimmsten Falle eben alles miteinander vernetzt ist – in einem einzigen Netzwerk.



Aktuelle Entwicklungen

Trotz steigender Investitionsbereitschaft im Bereich der IT-Sicherheit kommt es dennoch immer wieder zu erfolgreichen Ransomware-Angriffen. Dabei spielt es keine Rolle, wie klein oder unbekannt ein Unternehmen ist – jedes Unternehmen ist ein potenzielles Ziel. Die professionellen Angreifer-Gruppen bedienen sich gerne des Gießkannen-Prinzips und adressieren beliebig viele E-Mail-Konten über die Spam-Verteiler. Die Mechanismen des Angriffs entwickeln sich ständig weiter, so dass es trotz massiver Investitionen in IT-Security Software keine 100%ige Sicherheit gibt.

Mögliche Folgen eines erfolgreichen Angriffs:

- Betriebsstillstand
- Vertrauensverlust
- Erhöhte Mitarbeiterfluktuation
- Vertragsstrafen
- Stillstand statt Weiterentwicklung

Zwar gehen die wenigstens Unternehmen in Folge eines Vorfalls in die Insolvenz, jedoch wirft es das Unternehmen Monate zurück und der Wettbewerb hat die Möglichkeit aufzuholen.

Investitionen – nicht nur, sondern auch wegen NIS2

Damit ich davon verschont bleiben muss ich investieren. Das sagt nicht nur die suresecure als Berater für IT-Sicherheit, sondern auch die Europäische Union, die mit NIS2 eine Direktive auf den Weg bringt, um die digitalen und kritischen Infrastrukturen Europas resilienter gegen Cyber-angriffe zu machen. Über 30.000 Unternehmen in Deutschland werden mutmaßlich ab März 2025 davon betroffen sein. Die Anforderungen der NIS2-Direktive sind ziemlich konkret und gehören zu der Grundausstattung im Bereich der Cyber-Abwehr.

Dennoch erfüllen die meisten Unternehmen in Deutschland die Anforderungen nicht. Kommt es zu einer Prüfung oder einem Sicherheitsvorfall, kann ich als Geschäfts-führer demnächst auch noch persönlich haftbar gemacht werden.

Positiv ist, dass viele Unternehmen hier bereits einen Handlungsbedarf entdeckt haben. Obwohl in einigen Unternehmen bereits Budget und Roadmaps abgestimmt werden, wird die Umsetzung der Maß-nahmen noch einige Zeit erfordern. Denn den größten Mangel haben die Unter-nehmen nicht bei dem Einsatz von Technologie, sondern bei der Einstellung von Fachkräften.

Fachkräfte(m)-Angel:

Cybersecurity Spezialisten sind begehrt und zählen zu den Spitzenverdienern in der IT-Branche. Das führt dazu, dass sie sich den Arbeitgeber und die Arbeitsbedingungen aussuchen können. Das bedeutet, dass ich als Geschäftsführer zwar Planstellen freigeben kann, aber diese oftmals lange Zeit unbesetzt bleiben können. Gründe dafür sind u. a. Standortnachteil, Home-Office, Gehalt oder aber auch die berufliche Perspektive. Zudem reicht es nicht aus, die Stellen einmalig zu besetzen. Ich muss auch dafür Sorge tragen, dass die Experten erhalten bleiben und Vertretungsregelungen existieren.

Aus Sicht der Geschäftsführung ergeben sich daraus sechs Kernfragen, die man sich stellen sollte:

- **Wie schaffe ich es, den Status-Quo meiner Cybersecurity zu ermitteln, ohne dass ich viel Wissen aufbauen muss?**
- **Wie schaffe ich es, Informations-sicherheit messbar zu machen?**
- **Wie kann ich sicherstellen, dass Cyberangriffe 24x7 erkannt werden und darauf angemessen reagiert wird?**
- **Was kann ich tun, um trotz des Fachkräftemangel ausreichend Know-How zur Verfügung zu haben?**
- **Welche Maßnahmen muss ich priorisieren, um NIS2-konform zu sein bzw. nicht Opfer einer Ransomware-Attacke zu werden?**
- **Wie können diese Maßnahmen wirtschaftlich angemessen umgesetzt werden?**

Wie schaffe ich es, den Status-Quo meiner Cybersecurity zu ermitteln, ohne dass ich viel Wissen aufbauen muss?

Damit ich ein Verständnis für die aktuelle Situation bekomme, ist eine Bestands-aufnahme zwingende Notwendigkeit. Dazu beginne ich am besten erstmal mit einem Assessment. Diese können gegenüber Prüfern als Dokumentation für die intensive Auseinandersetzung mit Cybersecurity herangezogen werden.

Das Assessment sollte unbedingt von einem erfahrenen Dienstleister durch-geführt werden. Gerade die Erfahrung bringt einen enormen Mehrwert in jedes Assessment, denn der oder die Prüfende stellt an den richtigen Stellen die richtigen Zusatzfragen.

Der Projektinhaber ist ebenfalls für ein objektives Ergebnis wichtig. So kann ein internes Audit über z. B. den IT-Leiter auch dafür sorgen, dass gewisse Schwachstellen ganz bewusst nicht aufgedeckt werden.

Eine Innenrevision mit etwas IT-Affinität könnte hier in Frage kommen oder eben ein externer Dienstleister. Aber Achtung bei externen Dienstleistern: Diese neigen teilweise dazu, die Preisvorstellungen deutlich zu überziehen. Die Spanne liegt zwischen Workshops an zwei Tagen bis zu sechsstelligen Beratungsprojekten.

Meine persönliche Empfehlung: Mit etwas weniger anfangen. So lernt man den Prüfer kennen und kann auf dieser Basis das Engagement weiter ausbauen. Außerdem sollte ein Audit regelmäßig stattfinden, damit festgestellt werden kann, ob durch eventuelle Optimierungen bereits eine Verbesserung eingetreten ist.

Wie schaffe ich es, Informationssicherheit messbar zu machen?

Leider ist das nicht so einfach, aber es gibt eine Vielzahl von KPIs und theoretischen Ansätzen. In den USA ist es beispielsweise aktuell ein Trend, den potenziellen finanziellen Schaden durch einen Cyberangriff zu simulieren. Die Herausforderung dabei ist, dass dies meist durch eine KI auf generischen Werten basiert. Um das tatsächlich simulieren zu können, müssten wesentlich detaillierte Information über das Kerngeschäft herangezogen werden.

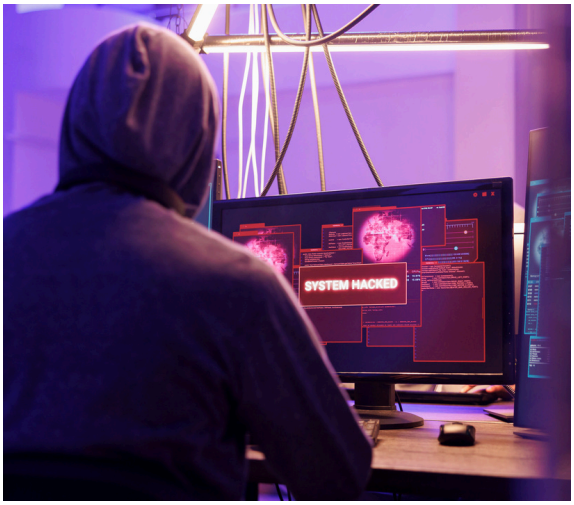
Einen anderen Ansatz stellt die Beobachtung der eigenen Angriffsfläche dar. Dies nennt man External Exposure Managment. Ich sehe meine IT so, wie sie der Angreifer sieht und vergleiche es möglicherweise noch mit anderen Infrastrukturen. Mein Haus muss nur sicherer sein als das des Nachbarn und eventuell steigt der Einbrecher dann lieber dort ein. Für die Beobachtung der External Exposure brauche ich auch kein zusätzliches Personal, denn dafür gibt es automatisierte Softwarelösungen, die das per Knopfdruck für mich oder beispielsweise auch meine Lieferanten ermitteln. So kann ich sehen, welche Schwachstellen meine von außen erreichbaren Systeme haben. Oder aber ob schon administrative Zugänge zu meiner IT im Darknet verfügbar sind. Denn diese werden im Darknet tagtäglich zum Verkauf angeboten.

Zusätzlich dazu kann ich auch KPIs für meine interne Infrastruktur erheben beispielsweise, wie viele Schwachstellen habe ich pro IT-Asset? Oder aber die Bemessung der abgewehrten Angriffe. Viele schauen sich das nicht an, weil die Angriffe ja sowieso abgewehrt wurden. Tatsächlich lässt sich durch diese Zahlen aber ein Lagebild erstellen. In Zeiten von Ransomware, in denen regelmäßig komplette IT-Infrastrukturen verschlüsselt werden, macht es definitiv auch Sinn, KPIs zu den Backups zu ermitteln. Wie groß ist der Zeitabstand zwischen zwei Backups? Wie lange dauert es im Durchschnitt eines Systems aus dem Backup wiederherzustellen?

Denn sollte die Ransomware zugeschlagen haben, dann sollte ich besser Backups haben, die nicht so weit zurückliegen und auch die Zeiten zur Wiederherstellung sollten so gering wie möglich sein. Denn jede Stunde, die der Betriebsstillstand länger anhält, kostet eine Menge Geld.

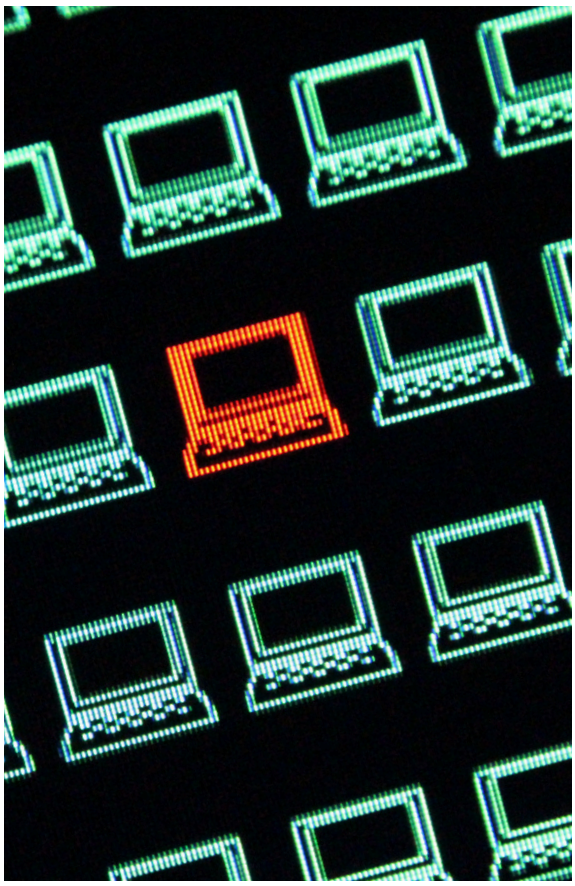
Wie kann ich sicherstellen, dass Cyber-angriffe 24x7 erkannt werden und darauf angemessen reagiert wird?

Angriffe finden rund um die Uhr statt, vor allem aber an Feiertagen und Wochenenden. Denn die Angreifer kennen unsere Büroarbeitszeiten. Ein erfolgreicher Cyberangriff findet nicht in wenigen Stunden statt. Bis zur Ausführung der Ransomware befindet sich die Angreifer-Gruppe bereits monatelang im Netzwerk, um den Roll-Out und die Erpressung vorzubereiten. Nur so können die Cyber-kriminellen sichergehen, dass die Verschlüsselung nicht unterbunden wird.



Montagmorgens im Büro erwartet einen dann die unangenehme Überraschung. Die Angreifer können hier meist unbeobachtet agieren, weil viele Unternehmen nicht in der Lage sind, die sicherheitsrelevanten Ereignisse rund um die Uhr zu überwachen. Damit das möglich ist, wird ein SOC (Security Operations Center) benötigt, . Das SOC besteht aus Technologie, Menschen und Prozessen. In der Regel ist es nicht wirtschaftlich für den Mittelstand dies selbst zu betreiben.

Viele unterschätzen die Aufwände, was dazu führt, dass das eigene SOC entweder niemals etabliert wird oder aber hinter den Anforderungen zurückbleibt. Sinnvoller und üblich ist es für solche Dienste Service Provider zu beauftragen. Diese betreiben große SOCs und bieten diese als Services für den deutschen Mittelstand an. Erfolgreich angegriffen wird jeder, die Kunst ist es, Angreifer frühzeitig zu entdecken und abzuwehren, bevor ein großer Schaden entsteht. Hierbei spielt auch gut ausgebildetes Personal und erprobte Prozesse eine große Rolle. Was bringt mir die Alarmierung "Alarmstufe Rot", wenn niemand weiß, was in dem Fall zu tun ist.



Was kann ich tun, um trotz des Fachkräftemangel ausreichend Experten zur Verfügung zu haben?

Es gibt verschiedene Ansätze dem Fachkräftemangel entgegen zu wirken. Manche davon, wie z. B. das interne Ausbilden von Talenten oder gezieltes Recruiting, sind eher mittel- bis langfristig ausgelegt.

Schnelle Verfügbarkeit von Expertise gibt es häufig nur extern in Form von Dienstleistern. Das kann ein IT-Systemhaus als Service-Partner für die IT-Infrastruktur sein, aber auch ein CISO as a Service, der für die strategische Entwicklung der Cyber-Resilienz die Verantwortung trägt.

Nicht selten hört man den Satz "Cyber-Security ist Chefsache". Das muss mir bei der Auslagerung von Tätigkeiten bewusst sein. Auch ein Dienstleister braucht einen Sparrings- oder Ansprechpartner, um die gewünschte Leistung erbringen zu können. Das kann der Chief Information Security Officer oder auch ein IT-Leiter oder Security Manager sein. Dieser arbeitet den Dienstleistern zu und setzt die Interessen des Unternehmens durch. Die Steuerung und Kontrolle bleiben dadurch im Unternehmen und die operativen Tätigkeiten können ausgelagert werden.

Bitte aber immer prüfen, ob die Personen oder Institutionen fachlich in der Lage sind, den Anforderungen gerecht zu werden. Ein IT-Administrator ist noch lange kein Security Analyst, auch wenn beide in der IT arbeiten. Das wäre so, als würde ich den Dachdecker meine Fliesen im Bad legen lassen. Das kann funktionieren, muss aber nicht. Auch einen Werksstudenten damit zu beauftragen, eine globale Security Strategie umzusetzen, ist aus meiner Sicht nicht fair gegenüber dem Mitarbeitenden und das Ergebnis wird nicht zufriedenstellend sein.

Welche Maßnahmen muss ich priorisieren, um NIS2 konform zu sein bzw. nicht Opfer einer Ransomware-Attacke zu werden?

Wenn ich mich als Geschäftsführer mit den notwendigen Maßnahmen auseinandersetze, dann werde ich schnell erschlagen. Sowohl von der Menge als auch den Begrifflichkeiten. Wenn ich mich dann im Markt umhöre, schreit jeder "kauf meine Software und dann bist du NIS2 Compliant". Zum Glück handelt es ich hierbei nur um leere Marketingversprechen und keine Rechtsberatung. Ja, es kann sein, dass eine Software angeschafft werden muss. Aber genauso wie im Handwerk bringt mir der Hammer ohne das entsprechende Personal mit Erfahrung und Abläufen gar nichts. Im Kern muss ich mich erstmal mit 2 Dingen beschäftigen:

- **Bin ich in der Lage 24x7 Angriffe zu erkennen und angemessen zu reagieren?**
- **Habe ich in meiner Unternehmung Richtlinien erlassen um Cyber-Risiken zu mitigieren?**

Bezüglich der unternehmensweiten Richtlinien gibt es Best-Practices und Frameworks, auf die wir zurückgreifen können. Ein ISMS - Information Security Management System nach ISO 27001 hat die Aufgabe, Richtlinien zu etablieren, die regelmäßig überprüft und überarbeitet werden.. Diese definierten Richtlinien sind die Grundlage für die meisten Maßnahmen, die auch von NIS2 gefordert werden. Für die technische Umsetzung wird dann eventuell noch etwas Software benötigt, ist aber nicht immer zwingend notwendig.

Wie können diese Maßnahmen wirtschaftlich angemessen umgesetzt werden?

Cybersecurity kostet Geld. Die Empfehlung des BSI lautet: 15 % des IT-Budgets sollte in Cybersecurity-Maßnahmen investiert werden. Das bedingt natürlich, dass das IT-Budget in Relation zum Umsatz angemessen ist. Mittlerweile gibt es aber einen erkennbaren Trend, der das Security-Budget gar nicht mehr an das IT-Budget koppelt, da die Informationssicherheit kein reines IT-Thema ist.

Dazu muss einem bewusst sein, dass die meisten Unternehmen in Deutschland nicht mal den Mindeststandard etabliert haben. Das heißt, ich muss erstmal ordentlich investieren, um auf den Status-Quo zu kommen.

Denn ich habe Schulden aus der Vergangenheit aufgebaut. Ich kann mich auch entscheiden, nicht zu investieren und dann hoffen, dass ich nicht erfolgreich angegriffen werde. Meine Erfahrung aber aus all meinen bisherigen Sicherheitsvorfällen ist: Die hohen Schäden wären mit überschaubaren Investitionen alle verhindert worden. Meine Empfehlung ist es zunächst eine Zieldefinition anzusetzen und dann zu überlegen, wie komme ich dahin.

Ein Beispiel:
Ich möchte, dass alle meine weltweit verteilten Produktionsstandorte 24x7 überwacht werden, damit es nicht zu einem Betriebsausfall kommt. Wir erinnern uns, bei einem SOC benötigen wir Menschen, Prozesse und Technologien.

Ich muss mich also fragen: Bin ich in der Lage, ein Team von min. 10 Security-Experten aufzubauen und zu halten? Bin ich in der Lage die notwendigen Prozesse zu etablieren? Haben die Experten die notwendige Erfahrung, dass diese Prozesse auch zielführend sind? Welche IT-Assets besitze ich in der Produktion? Sehr wahrscheinlich wird IT, OT und auch IoT eingesetzt. Welche Technologie wird benötigt, um das abzudecken?

Das sind eine ganze Menge Fragen, die da aufkommen. Allerdings habe ich andersherum schon zu viele Projekte scheitern sehen. Der andere Weg wäre, zu schauen was bereits vorhanden ist und das Beste daraus zu machen. Im Ergebnis wird aber dann oft das Ziel nicht erreicht bzw. die Kosten werden noch höher, weil Fehlinvestitionen getätigt werden.

Key-Take-Aways:

- Eine Cybersecurity-Strategie beginnt mit einer Bestandsaufnahme
- Ein strategischer Ansatz schafft Planungssischerheit
- Die eigene Verteidigungsstärke gegen Cyberangriffe sollte einem bewusst sein
- Cyber-Resilienz als Wettbewerbsvorteil verstehen

Zusammenfassung

Als Geschäftsführer oder Mitglied der Geschäftsleitung steht man in der Verantwortung, die eigene Cyber-Resilienz sicherzustellen. Wer dieser Verantwortung nicht nachkommt, riskiert perspektivisch eine persönliche Haftung.
Um dieser Aufgabe gerecht zu werden, ist weniger das Know-how als vielmehr die Priorisierung entscheidend. Aus der Position heraus kann ich dafür sorgen, dass die Informationssicherheit auf der C-Level Agenda steht und dort auch regelmäßig besprochen wird. Es ist enorm wichtig, sich ein paar grundlegende Dinge reporten zu lassen, ohne zu tief ins Detail zu gehen. Jedoch sollte es immer so sein, dass das C-Level ein Gefühl für die eigene digitale Verteidigung hat.

Weitere Informationen zum Thema:

Podcast-Folge:

Mit Cyberaudit und IT
Sicherheit auf der sicheren Seite

Whitepaper:

Cyberaudit
Mit vereinten Kräften zur Resilienz

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de