Auszug aus tribune November 2022
Das Magazin mit unternehmerischen Visionen
Handelskammer beider Basel
Advokatenkammer Basel
Jubiläumsstiftung La Roche & Co.

«Cyber Security muss 365 Tage im Jahr ein Thema sein!»

Mathias Bücherl
Chief Technology Officer
Axians IT Services AG
mathias.buecherl@axians.com

In der 1. Industrienacht der Regio Basel gehörte das IT/OT Security Operations Center (SOC) des ICT-Dienstleistungsunternehmens Axians in uptownBasel bei Arlesheim zu den meistbesuchten Attraktionen. In einer hochmodernen Kommandozentrale, die an diejenige des Raumschiffs Entreprise erinnert, sorgen hier hoch qualifizierte Informatikerinnen und Informatiker rund um die Uhr für den Schutz von Unternehmensnetzwerken vor Hackerangriffen. «tribune» hat dort den Mann getroffen, der für den Aufbau und den Betrieb dieses Zentrums mitverantwortlich zeichnet.

Mathias Bücherl, was ist Ihr Kerngeschäft als Chief Technology Officer?
Axians Cyber Security bietet sogenannte Managed Security Services an. In diesem Bereich überwachen und schützen wir Systeme nach dem Prinzip «Identify – Protect – Detect – Respond – Recover». Wir *identifizieren* Datenbestände und die Risiken, denen sie ausgesetzt sind. Dann fragen wir uns, wie die Daten *geschützt* werden müssen. Auf Stufe *Detect* sorgen wir dafür, dass wir schnellstmöglich merken, wenn ein Schaden droht. Dann wird reagiert – *Respond* –, und schliesslich geht es um die *Wiederherstellung* des Normalzustands. Wir bieten unseren Kunden so eine Rundummöglichkeit, sich zu schützen.

Was geht hier in diesem Raum vor?
Das SOC kümmert sich um die Bereiche Detect, Respond und Recover. Hier sammeln unsere Analystinnen und Analysten Daten aus den Unternehmensnetzwerken unserer Kunden. Sie sehen auf den Bildschirmen sofort, wo ein unvorhersehbares Ereignis eintritt und agieren dann wie die Piloten von Flugzeugen in einer aussergewöhnlichen Lage: Sie arbeiten eine Checklist ab, um die Störung zu beseitigen und den Normalzustand wieder herzustellen. Danach folgt die Aufarbeitung. Was ist passiert? Weshalb ist es dazu gekommen?

«Cyber Security ist in erster Linie ein Gedankenweg.»

Und wie kann das Unternehmen solche Zwischenfälle künftig verhindern? Das ist unser Job im SOC im Rahmen von Managed Services: Wir machen unsere Kunden sicherer in allen Belangen der Informatik und der Informationstechnologie.

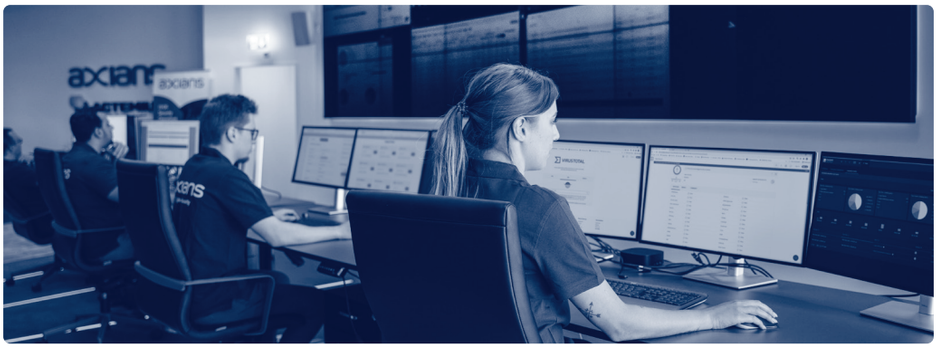
Beziehen die Kunden Sie von Anfang an mit ein? Oder werden Sie erst zu Hilfe gerufen, wenn «das Triebwerk schon brennt»?
Letzteres kommt leider sehr häufig vor. Dann übernimmt das Incident Management aus dem Bereich Response. Diese Feuerwehr rückt aus, im besseren Fall, wenn das Flugzeug noch in der Luft ist, und gibt den Piloten beziehungsweise den IT-Fachleuten der Kunden Anweisungen, wie es sicher gelandet werden kann. Im schlechteren Fall, wenn der Absturz Tatsache ist, setzen unsere Fachleute die noch vorhandenen Bruchstücke so gut wie möglich wieder zusammen und retten, was noch zu retten ist.

Welche Fehler führen hauptsächlich zu IT-Problemen in Unternehmen?
Das Internet und ganz speziell die E-Mail-Kommunikation sind Einfallstore in jedes System. Ungeschützt machen sie Angreifenden Datendiebstahl und Sabotageakte leicht. Mit dieser Tatsache beschäftigen sich viele Mitarbeitende kaum und leider auch Führungskräfte oft zu wenig. Sie wissen zwar um die Problematik, aber sie verschliessen die Augen, nicht selten, weil Sicherheit im Netz nicht gratis zu haben ist. Das Risiko wird unterschätzt – frei nach dem Motto «Uns kann das nicht passieren» – oder allenfalls an eine Versicherung delegiert. Ein Unternehmen muss aber nicht nur das Risiko erkennen – und ein solches ist immer da! – seine Führung muss es auch richtig einstufen und frühzeitig die richtigen Massnahmen einleiten. In dieser Verpflichtung sind Geschäftsführung und Verwaltungsräte. Wenn diese nach eingehender Prüfung zum Schluss kommen: «Okay – es gibt Cyberangriffe, aber ich akzeptiere das Risiko» – dann ist das ein mögliches «Mindset». Mit anderen Worten: Cyber Security ist in erster Linie ein Gedankenweg; erst danach eine technische Herausforderung.

Hat sich dieses Mindset in letzter Zeit verändert?
Der Geschäftsbereich Cyber Security wächst in der Tat, und dies sicher auch, weil die feindlichen Angriffe auf Netzwerke zunehmen. Das Umdenken ist in vollem Gang; in den letzten Jahren haben viele Unternehmen gemerkt und teilweise auch schmerzlich erfahren müssen, dass sie die Augen nicht mehr vor der Gefahr verschliessen und vor allem Security nicht länger mit Safety gleichsetzen können. Safety im Sinn von Betriebssicherheit steht bei allen Unternehmen zuoberst auf der Checklist, weil sie wissen: Eine

Über Axians

Axians ist die globale Marke für ICT von VINCI Energies und beschäftigt 12'500 Spezialistinnen und Spezialisten in 27 Ländern weltweit. Axians Schweiz ist ein agiles Unternehmensnetzwerk aus spezialisierten ICT-Dienstleistern und Softwareherstellern an über 20 Standorten in allen Schweizer Sprachregionen. Das IT/OT Security Operations Center (SOC) von Axians befindet sich im neuen Kompetenzzentrum für Industrie 4.0 «uptown Basel» am Schorenweg in Arlesheim.



unsachgemäss installierte oder bediente Stanzmaschine kann einen Menschen seinen Arm kosten. Im Cyber Security-Bereich fehlt dieses Verständnis häufig. Ein Netzwerkkabel sieht halt nicht so gefährlich aus wie eine Kreissäge, aber es kann eine ganze Produktion lahmlegen. Und während der Safety-Punkt nach der sicheren Installation der Maschine und der Abgabe von Helmen ans Personal meist abgehakt werden kann, ist Cyber Security nie erledigt.

Was können Ihre Spezialisten retten, wenn nichts mehr geht in einem Firmennetz?
Das ist stark abhängig davon, wie das Unternehmen auf einen solchen Fall vorbereitet ist. Das nennen wir Business Continuity Management beziehungsweise Desaster Recovery. Da geht man zum Chef und fragt: «Hast du diese Pläne? Ist dir bewusst gewesen, dass das passieren kann?» Viele Unternehmen machen zwar Backups, aber sie testen sie nicht. Oder sie haben keine Dokumentation erstellt und alles Wissen ist ausschliesslich im Kopf einer einzelnen IT-Fachkraft abgespeichert. Ein solcher Wiederaufbauprozess ist um vieles leichter, wenn sich jemand schon vorher Gedanken darüber gemacht hat. Sonst wird die Bewältigung eines solchen Desasters schwierig bis unmöglich. Vor diesem Fall stehen wir oft im Bereich Cyber Security. Und da möchte ich an die Unternehmen appellieren: Es ist weder ein extrem schwieriges noch ein komplexes technisches Thema. Aber man muss sich ihm öffnen und sich mit ihm befassen.

Wie sieht die Interaktion zwischen den Angreifern und Ihnen als Verteidiger aus?
Das ist ein ständiges Wettrüsten. Wir auf unserer Seite halten uns über Taktiken und Techniken der Angreifenden auf dem Laufenden, auch mit Mitteln der künstlichen Intelligenz. Weiter stellen wir sogenannte «Honeypots» in ein Netzwerk; das sind Systemteile, die viele Schwachstellen aufweisen. Mit einem solchen Honigtopf provozieren wir einen Angriff auf ein System, das natürlich isoliert ausserhalb des Unternehmens liegt, damit nichts passieren kann. So lernen wir die Methoden der Angreifer kennen und merken, wenn sich ein Ernstfall anbahnt. Eine weitere Möglichkeit ist die Analyse von bereits erfolgten Angriffen auf andere Unternehmen; da tauschen wir uns regelmässig mit anderen Spezialisten aus.

> «Auch unsere Branche leidet unter einem Mangel an Fachkräften.»

Gibt es die einhundertprozentige Sicherheit im Cyber-Space?
Nein. Was vom Menschen geschaffen wird, ist fehlerhaft und angreifbar. Es gibt 365 Tage im Jahr neue und andere Möglichkeiten, ein IT-System anzugreifen. Kein Spezialist und schon gar kein Laie kann also sagen, dass der Cyber Security-Job für dieses Quartal erledigt sei und das Thema in zwölf Monaten wieder auf die Traktandenliste komme. Wer aber sein Mindset justiert und erkannt hat, dass Cyber Security eine 365-Tage-im-Jahr-Aufgabe ist, der kommt mit seiner IT-Sicherheit nahe an die 100 Prozent heran.

Gibt es genügend Spezialisten, die sich auf diese komplexen Aufgaben verstehen?
Auch unsere Branche leidet unter einem Mangel an Fachkräften. Das hat auch damit zu tun, dass man ein Konzept zuerst von Grund auf verstehen muss, bevor es sicherer gemacht werden kann. Mit anderen Worten: Cyber Security ist eine zusätzliche Stufe der Ausbildung. Deshalb bleiben viele Nachwuchsinformatiker bei der Anwendungsentwicklung. Sie haben ein abgeschlossenes Studium und eine Stelle in einem gut bezahlten Beruf auf sicher: Weshalb soll sich da einer – oder eine – noch ein weiteres Studium obendrauf packen? Apropos «eine»: In der Informatik finden wir gerade einmal 14 Prozent Frauen. Bei der Personalrekrutierung setzen wir daher stark auf Diversität, nicht nur was das Geschlecht betrifft. Wir akquirieren auch talentierte und motivierte Leute aus völlig fachfremden Gebieten. Nicht selten finden wir dabei Köpfe, die «out of the box» denken können und völlig neue Ideen einbringen.

Vielen Dank, Herr Bücherl, für dieses Gespräch.

Interview: Roger Thiriet

Mathias Bücherl
ist Chief Technology Officer von Axians IT Services AG. Er verfügt über langjährige Erfahrung im Bereich Managed Cyber Defense und Security Operation und hat in dieser Eigenschaft das Security Operations Center von Axians in Basel/Arlesheim aufgebaut. Neben seinem beruflichen Engagement ist er als Dozent für Cyber Security an der Hochschule Luzern und der Dualen Hochschule Baden-Württemberg DHBW in Stuttgart tätig.