CYBER-SICHERHEIT

CISO, EIN BERUF AUF MESSERS SCHNEIDE

Victor Poitevin
Digital Manager,
Stormshield

Sie haben die Krise selbst bezahlt. An der Frontlinie scheint sich mit der Covid-19-Krise das Unbehagen der CISO, die zwischen drängenden internen Forderungen und langfristigen Sicherheitserfordernissen hin- und hergerissen sind, noch verschärft zu haben. So sehr, dass das Thema Burn-Out heute in der Branche kein Tabu mehr ist. Analyse.

Im November 2019 zeichnete die *„CISO Stress"*-Umfrage unter mehr als 800 Sicherheitsmanagern für Informationssysteme (CISO) und Führungskräften in den Vereinigten Staaten und im Vereinigten Königreich ein düsteres Bild eines der heute am meisten gefragtesten Arbeitsplätze. Und zwar mit alarmierenden Zahlen: 88 % der befragten CISO betrachten sich selbst als *„mäßig oder extrem gestresst"*, wobei 48 % erklären, dass ihr Stresspegel Auswirkungen auf ihre psychische Gesundheit hat, 23 % geben zu, dass sie zu Medikamenten oder Alkohol gegriffen haben. Lange Arbeitszeiten, knappe Budgets, Schwierigkeiten beim Rekrutieren und ein gewisser Mangel an Vertretung in den Verwaltungsräten; die Situation ist nicht sehr rosig - auch wenn Mitarbeiter und Betriebsteams immer mehr Geschwindigkeit und Beweglichkeit bei IT-Tools fordern. Dazu kommt ein ständiger Stress angesichts der schnelleren neuen Cyber-Bedrohungen, mit der Angst, zur Verantwortung gezogen zu werden, wenn etwas schief geht... **Wie steht es also um die psychische Gesundheit der CISO?** Was kann man tun, um die Situation zu verbessern?

DIE KULTUR AN DER WURZEL DES PROBLEMS

Vor allem die CISO leiden darunter, missverstanden zu werden. Yohann, der nach dem Ausscheiden aus seiner vorherigen Position eine Stelle sucht, um Burn-out zu vermeiden, sagt: *„Frustrierend ist, dass man es nicht sieht, wenn man seine Arbeit gut macht."* In diesem Zusammenhang ist es schwierig, sich als Cyber-Sicherheitsexperte zu bewähren... Die Arbeit der CISOs ist jedoch eine Arbeit für Menschen, die sich für neue Technologien begeistern, für die sich viele über ihre Arbeit hinaus engagieren. *„Das Gebiet der IT-Sicherheit ist so groß, dass wir nie genug tun können. Wir tun es aus Berufsethik und Liebe zu unserer Arbeit, aber es kann anstrengend werden"*, fährt er fort. Die *„CISO Stress"*-Studie unterstreicht das Gewicht dieser Verantwortung für diese IT-Sicherheitsexperten: bei 44 % der Befragten ist der Hauptgrund für ihr Unbehagen die Tatsache, dass sie die Cybersicherheit ihres Unternehmens tragen, in einer Welt, die die Tragweite der Probleme, mit denen sie konfrontiert sind, nicht anerkennt. So ist das Stressniveau bei 35 % der Befragten so hoch, dass es sich auf ihre körperliche Gesundheit auswirkt... Nach ihrer Veröffentlichung stieß die Studie auf ein starkes Echo, und **Russell Haworth**, CEO von Nominet und Sponsor der Studie, berichtet, er habe zahlreiche Nachrichten von CISO und Cybersicherheitsexperten erhalten, die sich in den Umfrageergebnissen wiederfinden

„Das Feld der IT-Sicherheit ist so groß, dass wir nie genug tun können. Wir tun es aus Berufsethik und Liebe zu unserer Arbeit, aber es kann anstrengend werden."

Die Studie stützte sich auf Fachleute in den Vereinigten Staaten und im Vereinigten Königreich, aber die Lage scheint kaum besser, wenn man Frankreich ansieht. Die Problemstellungen unterscheiden sich jedoch je nach kulturellen Besonderheiten... Frankreich soll tatsächlich die Profile der *„Fachleute"* sehr wenig würdigen. **Alice Louis,** IP/IT-Rechtsanwältin und Expertin für die Verwaltung der Informationswerte, erinnert an das Beispiel **Louis Pouzin**. *„Als brillanter Forscher, Ingenieur und Polytechniker ist er weltweit als einer der Gründerväter des Internets anerkannt. Das Projekt „Cyclades", das er in den 1970er Jahren leitete, führte zu beträchtlichen Fortschritten auf dem Gebiet der Netzwerkarchitektur. Die Amerikaner, damals mitten im Kalten Krieg, verstanden schnell das strategische Interesse, während die französische Regierung beschloss, ins Minitel zu investieren... Ich bin fassungslos, wie wenig wir wissen, um Lehren aus der Vergangenheit ziehen zu können! Frankreich hat viele Talente; das französische Genie kommt auch in den Informations- und Kommunikationstechnologien zum Ausdruck."* Auf der anderen Seite des Atlantiks ist dies nicht der Fall. *„Schaut man sich die Top 10 der börsennotierten Unternehmen an, so werden drei Viertel von Ingenieuren und Programmierern geleitet. Dies ist absolut nicht der Fall in Frankreich, wo die Ingenieurkultur, auf die wir stolz sind, eher ein Hirngespinst ist. Tatsächlich gibt es keinen Polytechniker an der Spitze des Staates, sondern nur Enarchen"*, klagt **Fabrice Epelboin**, Unternehmer und Lehrer an der Sciences Po.

In seinen Augen wird die Informationstechnologie immer noch mit einer gewissen Verachtung betrachtet, worauf er provokativ reagiert: *„In den Unternehmen kennen die Leute den Namen des CIO nicht, er interessiert sie nicht. Für die großen französischen Unternehmen ist der CIO eine Putzfrau, sicher sehr gut bezahlt, aber in der Position eines einfachen Ausführenden, den man ruft, wenn man ein Problem hat*". Und was ist dann der CISO, der dem CIO unterstellt ist? In der Ausgabe 2018 der Clusif-Studie „*IT-Bedrohungen und Sicherheitspraktiken in Frankreich*" sind 77 % der CISO der größten Unternehmen tatsächlich dem CIO unterstellt. In Unternehmen mit weniger als 1000 Beschäftigten unterstehen 55 % von ihnen direkt der Geschäftsleitung.

In den Vereinigten Staaten und in den meisten englischsprachigen Ländern ist sein Pendant der **CISO (Chief Information Security Officer), der immer mehr Teil des Leitungsausschusses wird.** In Frankreich wird er innerhalb seines Unternehmens nicht wahrgenommen. *„Dies hat damit zu tun, dass der CISO im Grund ein Hacker ist. Er kommt nicht aus den Grandes Ecoles, die wir so sehr schätzen, er kennt nicht die Codes, sonst wäre er Ingenieur geworden*", fährt der Lehrer fort. Tatsächlich werden die CISOs lediglich als unterstützende Funktionen wahrgenommen...

CISOs IN DER KRISE VOR DER KRISE

Dies umso mehr, als der CISO isoliert ist, weit davon entfernt, von einem Relaissystem im Unternehmen zu profitieren, im Gegenteil... *„Es hat mit dem Organigramm zu tun*", erklärt Yohann. *„Wir werden als notwendiges Übel wahrgenommen. Unsere Aufgaben kollidieren nicht nur mit denen anderer Abteilungen, sondern auch mit denen des CIO, unseres N+1, dessen Ziele Verfügbarkeit der Infrastruktur und Fähigkeit, eine Last zu tragen, das Gegenteil von unseren sind.*" Wenn beide aufeinandertreffen, muss der CISO, der die Krümel des Budgets und ein oft kleines Team hat, manchmal im Namen geschäftlicher Notwendigkeiten mit Sicherheitsverletzungen zurechtkommen....

„Die CISOs werden als notwendiges Übel wahrgenommen."

Jérémy, ein weiterer CISO, der sich bereit erklärt hat, Stellung zu nehmen, stimmt dem zu. *„Wir sind in einer Zwickmühle zwischen dem CIO, dem Leitungsausschuss und den Anwendern, die nicht verstehen, warum wir Sicherheitsstandards festlegen. Um in die Richtung der CIO zu gehen, müssen wir oft gefährliche Situationen validieren und laufen Gefahr, dass es auf uns zurückfällt.*" Mit einem gezwungenen Lachen führt er ein bekanntes Sprichwort unter CISOs an: *„Der CIO ist die Sicherung für das Management, der CISO die Sicherung für den CIO*". Wenn es ein Problem gibt, wird der CISO umgehend beschuldigt, sogar geopfert.

„Die CISOs sind in einer Zwickmühle zwischen dem CIO, dem Leitungsausschuss und den Anwendern, die nicht verstehen, warum wir Sicherheitsstandards festlegen."

Dieser schwierige Zustand wurde durch die Covid-19-Krise verschärft, was die Reibungen noch verstärkte. „*Das einzige Ziel einiger Comex besteht jetzt darin, zu überleben, und das geht zu Lasten der Sicherheitsstandards, für die wir eintreten*“, sagt Jérémy. Die Einführung der Telearbeit für das gesamte Unternehmen durch die Systematisierung von BYOD hat viele Lücken in der IT-Sicherheit geöffnet und gleichzeitig die bereits übervolle Arbeitslast der CISO vervielfacht. „*Von einem Tag auf den anderen musste alles geändert werden. Und kein Unternehmen war bereit*“, sagt Jérémy. „*Für die Mitarbeiter stand nichts auf dem Spiel, denn ihre Arbeit änderte sich nicht, während es für uns eine völlige Umgestaltung bedeutete.*“ Im Zuge dieser Praktiken entstehen neue Bedrohungen wie z. B. IT-Shadowing, die durch die Nutzung von Anwendungen und Diensten parallel zu denen der IT-Abteilung verursacht werden. „*Durch Anziehen gelang es den CISO jedoch, viele Initiativen schnell auf den Weg zu bringen. Dieser zweischneidige Erfolg hat die Komplexität und die Schwierigkeiten unserer Aufgabe unsichtbar gemacht...*“, sagt Jeremy.

Und der Preis, der für den Erfolg in diesem schwierigen Balanceakt zu zahlen ist, kann die Implosion des eigenen Lebens sein. „*Ich komme spät aus dem Büro nach Hause, esse schnell zu Abend und arbeite bis ein Uhr nachts weiter. Wochenenden kenne ich nicht mehr*“, sagt Yohann. In den englischsprachigen Ländern zeigt die „*CISO Stress*“-Studie das gleiche Unbehagen: 95 % der Befragten geben an, mehr zu arbeiten, als ihr Vertrag verlangt, und 39 % von ihnen haben bereits wegen ihrer Arbeit die Hochzeit eines Familienmitglieds oder den Urlaub verpasst.

WIE KÜMMERN SIE SICH UM IHRE CISO?

Sowohl intern als auch extern wird die CISO von allen Seiten angegriffen. Die CISO ist jedoch nicht zu ihrem Schicksal verdammt, und es sind verschiedene Lösungen zu erwägen.

Yohann und Jérémy sind sich einig. Die CISO darf nicht mehr dem CIO unterstellt sein. „*Dieser Bericht hindert den CISO daran, seine Rolle als Cybersicherheitsexperte und Gegenkraft, die er nur unabhängig ausüben kann, voll wahrzunehmen*“, erklärt Jérémy. Für ihn wäre es notwendig, von der amerikanischen Art zu lernen, die eher dazu neigt, Verantwortung zu delegieren. „*Der CISO muss auch so nah wie möglich am Top-Management sein und in den Comex integriert werden. Sobald er mit dem CIO auf Augenhöhe ist, kann er seine Positionen transparent verteidigen*“, fügt Yohann hinzu. Auf diese Weise würden die Schlichtungen in voller Kenntnis der Tatsachen erfolgen.

Eine Lösung für die Mitarbeiter könnte die Organisation von Bildungsworkshops sein. „*In den Köpfen der Mitarbeiter ist es einfach, Menschen in Telearbeit zu schicken. Sie verstehen nicht, dass damit ein anderes Netzwerk mit neuen Konzentrationsströmen geschützt werden muss. Wenn sie wüssten...*“, seufzt Yohann. Mit der Einführung von Workshops zur Sensibilisierung für digitale Hygiene würde man auch verstehen lernen, warum bestimmte gute Praktiken (nicht mehr nur ein achtstelliges Passwort,

nur die empfohlenen Werkzeuge verwenden usw.) notwendig sind. **In einer Zeit, in der die Grenzen zwischen Mitarbeitern und Fachkräften verschwimmen** und digitale Angriffe immer häufiger und raffinierter werden, haben die Mitarbeiter die damit verbundenen Risiken noch nicht vollständig begriffen. Nach der „*CISO Stress*"-Studie glauben nur 15 Prozent der Befragten, dass das Thema Cybersicherheit systematisch in den Unternehmen bei Treffen von Führungskräften behandelt wird... Der CISO, ein IT-Sicherheitsexperte, muss auch zum Pädagogen werden.

Ein weiterer von **Alice Louis**, die Interdisziplinarität befürwortet, favorisierter Weg ist „*das Steuern von Intelligenz-Netzwerken, insbesondere das von Ethik-Hackern*", die aus kultureller Sicht dem CISO näher stehen als dem CIO. Für die ersteren „*könnten sie wichtige Verbündete für Organisationen sein*", was dazu beitragen würde, das Kräfteverhältnis zugunsten der Cybersicherheit zu verschieben. Diese vertrauenswürdigen Hacker, auf die man manchmal eher hört, könnten heute in Unternehmen eine wichtige Rolle spielen und zu echten Erweiterungen der Sicherheitsteams werden. **Frans Rosén**, Hacker der HackerOne-Community, sagte übrigens Ende Mai in einer Pressemitteilung: „*Was mir am besten gefällt, sind die Reaktionen auf einige Bugs, die ich identifiziert habe. Wenn der CIO eines Unternehmens mich mitten in der Nacht anruft, um den Ernst der Lage zu verstehen, und in Panik gerät, wenn er die potenziellen Auswirkungen erkennt.*"

Yohann und Jérémy sehen zwar eine Verbesserung der Lage, aber sie fürchten die Rolle, die Covid-19 spielen könnte. Die Epidemie könnte die mageren Fortschritte bei der Art und Weise, wie die Rolle der CISO verstanden wird, rückgängig machen. Ist die Krise also ein Beschleuniger des Fortschritts oder ein Vektor, um die Uhr zurückzudrehen? Dazu ist es noch zu früh...
