STORMSHIELD

MEINUNGEN

# WELCHE MITARBEITER IN UNTERNEHMEN SIND ZIEL VON CYBERANGRIFFEN?

**Stéphane Prevost**
Product Marketing Manager, Stormshield

***„Das Problem liegt zwischen dem Stuhl und der Tastatur."*** **Diese Redensart, die (zu) oft in der IT- und Cybersicherheitsbranche verwendet wird, erinnert daran, dass eine der größten Cyber-Schwachstellen eines Unternehmens auf der Naivität seiner Mitarbeiter beruht. Aber ist es wirklich relevant? Und wer sind diejenigen, die am ehesten in die Falle von Cyberkriminellen tappen? Antwortelemente**

Im kollektiven Unterbewusstsein zielen Cyberangriffe auf einen Mitarbeiter, der in der Unternehmenshierarchie weit oben steht, da er Zugang zu sensiblen und kritischen Informationen hat. Dennoch erinnert **Sébastien Viou**, Direktor für Produktsicherheit und Cyber-Spezialist bei Stormshield, daran, dass *„diese wertvollen Ziele auch die am besten geschützten und vorsichtigsten sind"*. Deshalb *„handelt der Cyberkriminelle meist aus Opportunismus. Er greift dort an, wo sich die Schwachstelle in der Sicherheitskette* befindet". Was wäre, wenn hinter den offensichtlichen Profilen der Führungskräfte schließlich alle Mitarbeiter potenzielle Ziele wären?

# CYBERANGRIFFE AUF UNTERNEHMEN: WENN DER BAUER DIE DAME SCHLÄGT

Denn selbst ein Ziel mit begrenztem Zugriff auf die digitalen Ressourcen des Unternehmens kann zum ersten Meilenstein eines Cyberangriffs werden. Wie der Bauer, der auf einem Schachbrett so weit gehen kann, dass er die Dame umwirft. „*Die meisten digitalen Angriffe bewegen sich innerhalb des Unternehmensnetzwerks*“, sagt Sébastien Viou. *Ein Endgerät mit eingeschränkten Zugriffsrechten kann sehr wohl in ein trojanisches Pferd umgewandelt werden, um andere Endgeräte im Netzwerk zu infizieren, sodass Cyberkriminelle nach und nach immer größere Zugriffsrechte unterwandern können*“. Obwohl ein Mitarbeiter also keine wichtigen Berechtigungen im Informationssystem eines Unternehmens hat, ist er dennoch ein interessantes Ziel für Cyberkriminelle, wenn es um Seitwärtsbewegungen und die Erhöhung von Privilegien geht.

*„Es gibt immer noch sehr viele Unternehmen, in denen Mitarbeiter ohne ersichtliche Rechtfertigung Zugang zu kritischen Ressourcen haben. Für einige sind die Adminrechte ihrer Positionen wie soziale Errungenschaften.“*

**Sébastien Viou,** Direktor für Produktsicherheit und Cyber-Spezialist bei Stormshield

Und selbst das würde voraussetzen, dass die Unternehmen ihre Zugriffsrichtlinien ordnungsgemäß verwalten. Sébastien Viou stellt jedoch fest, „dass es immer noch sehr viele Unternehmen gibt, in denen Mitarbeiter ohne ersichtlichen Grund Zugriff auf kritische Ressourcen bekommen.Für einige sind die Adminrechte ihrer Positionen wie soziale Errungenschaften.“ Eine (andere) Realität, die das ungezielte Phishing zum wichtigsten Angriffsvektor im CESIN-Barometer 2021 macht: 80 % seiner Mitglieder waren im Jahr 2020 Opfer dieser Praxis. Ein leicht durchzuführender Cyberangriff, der es ermöglicht, die Anzahl der Versuche zu vervielfachen und auf die Masse der Mitarbeiterinnen und Mitarbeiter abzuzielen. **Cyberkriminelle setzen also auf Quantität, um die Statistik zu ihren Gunsten** zu beeinflussen: Früher oder später wird die Falle irgendwann bei jemandem im Unternehmen zuschnappen ... Schachmatt. Massive Angriffe also und für **Joseph Graceffa**, Präsident des Clubs für vernetzte Informationssicherheit (CLUSIR) Nordfrankreich, sogar erfolgreich. Er warnt davor, dass „*keine Person innerhalb der Zielorganisation vor Nachlässigkeit völlig sicher ist*“, auch nicht die vorsichtigsten Personen ...

Elemente, die leider eine Antwort auf die ursprüngliche Frage dieses Papiers ermöglichen. In Unternehmen können (und werden) alle Mitarbeiter Ziel von Cyberangriffen sein. Wie können Sie also verhindern, dass Sie sich in den Maschen verfangen?

# VON DER SENSIBILISIERUNG ZUR VERANTWORTUNGSÜBERNAHME DURCH DIE MITARBEITER/INNEN ÜBERGEHEN

Es ist zwar schwierig, eine allgemeine Analyse der Anfälligkeitsprofile aufgrund der Funktion der Mitarbeiter innerhalb eines Unternehmens vorzunehmen, **aber es scheint dennoch notwendig, die anfälligsten Mitarbeiter zu ermitteln**.

*„Durch Tests wird es möglich, die Personen ausfindig zu machen, die systematisch in die Falle tappen, die somit die schwächsten menschlichen Glieder in der Sicherheitskette sind."*

**Joseph Graceffa,** Präsident des Clubs für vernetzte Informationssicherheit (CLUSIR) Nordfrankreich

So nimmt Joseph Graceffa das Beispiel des Phishing: *„Es gibt heute sehr leicht zugängliche und kostengünstige Lösungen, um Tests zu automatisieren"*. Mit solchen Tools können Unternehmen Kampagnen programmieren, die sich selbstständig ausführen und gefälschte E-Mails mit bösartigen Inhalten an ihre Mitarbeiter senden. *„Durch Tests wird es möglich, die Personen ausfindig zu machen, die systematisch in die Falle tappen, die somit die schwächsten menschlichen Glieder in der Sicherheitskette sind.* Das Unternehmen kann also auf diese gefährdeten Mitarbeiter einwirken, *„angefangen damit, sicherzustellen, dass sie sich der möglichen Folgen ihres Verhaltens bewusst werden und in den Grundbegriffen der Cybersicherheit geschult werden"*. Viele Unternehmen führen **Sensibilisierungskampagnen und Schulungen zum Thema Cybersicherheit** durch, um ihre Mitarbeiter besser mit den Regeln der digitalen Hygiene vertraut zu machen. Sie werden außerdem von öffentlichen Einrichtungen wie der ANSSI stark dazu ermutigt, indem sie einen praktischen Leitfaden für Unternehmen anbietet, dessen erstes Kapitel den Titel *„Sensibilisieren und schulen"* trägt. Auf europäischer Ebene bezieht die Agentur der Europäischen Union für Cybersicherheit (ENISA) dieses Konzept der Sensibilisierung der Öffentlichkeit direkt mit in ihren Auftrag ein. Um dies zu erreichen, will die Institution *„die Mitgliedstaaten bei der Bewusstseinsbildung"* unterstützen, *„die Koordination zwischen den Mitgliedstaaten"* fördern und *„Verhaltenskodizes für Computerhygiene und digitale Kompetenz"* bereitstellen. Eine Strategie, die auch von Frankreich befürwortet wird. Nach dem Anstieg der Cyberangriffe, die während der Gesundheitskrise beobachtet wurden, bekräftigte Guillaume Poupard, Generaldirektor der ANSSI vor dem Senat, wie wichtig es ist, auf Ausbildung, Zertifizierung und die kontinuierliche Suche nach sektorspezifischen digitalen Hygieneregeln zu setzen: *„Die Einhaltung der Computerhygiene ist die Grundlage, sonst wäre es so, als würde man mit schmutzigen Händen einen hochpräzisen chirurgischen Eingriff durchführen wollen"*.

*„Die Einhaltung der Regeln der Computerhygiene ist die Grundlage, sonst wäre es so, als würde man mit schmutzigen Händen einen hochpräzisen chirurgischen Eingriff durchführen."*

**Guillaume Poupard,** Generaldirektor der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI) [in französischer Sprache]

Doch auch wenn er die Bedeutung der Sensibilisierung der Mitarbeiter als Antwort der Unternehmen auf Cyberrisiken nicht in Frage stellt, hält Sébastien Viou sie für „*völlig unzureichend, um sicherzustellen, dass die grundlegenden Regeln der digitalen Hygiene angewendet werden*". **Ist die Schlacht um das Cyberbewusstsein bereits verloren?** Die Versuchung, mit Ja zu antworten, ist groß, wenn man sich auf die in sozialen Netzwerken veröffentlichten Fotos von Geschäfts-PCs verlässt, die Personen an öffentlichen Orten zugänglich und unbeaufsichtigt gelassen haben. Für Sébastien Viou zeigt dies, dass es höchste Zeit ist, einen Gang höher zu schalten und **neben der Sensibilisierung auch eine Form der Verantwortungsübernahme durch die Mitarbeiter** einzuführen. „*Das Bewusstsein ist nicht verloren, heute ist die Mehrheit der Mitarbeiter für Cyberrisiken sensibilisiert, und das ist gut so. Sie wenden die Sicherheitsregeln jedoch trotz allem nicht an, weil sie fälschlicherweise davon ausgehen, dass das Risiko sie nicht betrifft*". Diese Verantwortungsübernahme könnte die Form annehmen, dass die Einhaltung der vom Unternehmen eingeführten Sicherheitsstandards und -regeln in das Aufgabenblatt des Mitarbeiters aufgenommen wird. „*So wäre das Risiko geteilt, da das Unternehmen im Falle eines nachgewiesenen schwerwiegenden Verstoßes hart durchgreifen könnte*". Diese Meinung teilt auch Joseph Graceffa, der darauf hinweist, dass diese Verantwortungsübernahme der Mitarbeiter bereits Realität ist, vor allem in großen angelsächsischen Unternehmen. „*Sie ergänzen in der Regel ihre Geschäftsordnungen mit einer IT-Charta und führen dann eine Sanktionsskala ein*", um je nach Schwere der Verfehlung ihrer Mitarbeiter hart durchgreifen zu können.

## EINEN BESSEREN ZUGANG ZUR CYBERSICHERHEIT GEWÄHRLEISTEN

Diese Verantwortungsübernahme muss jedoch mit einem besseren **Zugriff der Mitarbeiter auf Werkzeuge und Informationen zur Cybersicherheit** einhergehen. „*Da von ihnen verlangt wird, Verantwortung zu übernehmen, muss man ihnen sicherlich auch helfen, die Bedrohungen und deren Umfeld zu verstehen*", bestätigt Joseph Graceffa. Allerdings: „*Die Cybersicherheitslösungen des Unternehmens fallen traditionell in den Zuständigkeitsbereich der CISO-Teams. Und es wurde bis heute wenig unternommen, um die Nutzung für ein nicht spezialisiertes Publikum zu vereinfachen*". Eine leichter zugängliche und ergonomische (oder benutzerfreundliche) Cybersicherheitslösung könnte dazu beitragen, dass die Mitarbeiter des Unternehmens sie annehmen und ihre Kompetenzen erweitern.

Aus Sicht der internen Organisation **sollte die Personalabteilung eine stärkere Rolle in Bezug auf Fragen der Cybersicherheit spielen**. Das legt zumindest eine dedizierte Studie des Lehrstuhls RHO der Universität Freiburg und der CISEL Informatique SA nahe. Aufgrund ihrer traditionellen Zuständigkeiten wäre die Personalabteilung des Unternehmens am besten geeignet, das allgemeine Qualifikationsniveau der Organisation im Bereich der Cybersicherheit zu gewährleisten. Denn sie kann bereits in der Einstellungsphase je nach Profil Parameter der Cybersicherheitskultur einbeziehen. Da die Personalabteilung für die Schulungsprogramme der Mitarbeiter zuständig ist, kann sie auch am besten dafür sorgen, dass deren Wissen über Cybersicherheit ständig auf dem neuesten Stand ist (und zwar durch möglichst pädagogische Methoden, wie z. B. Tests). Zu diesem Zweck kann die Schaffung einer verstärkten Austauschstruktur zwischen der Personalabteilung und dem CISO sicherstellen, dass die Schulungsprogramme mit den Realitäten vor Ort übereinstimmen. Schließlich ist die Personalabteilung (in Verbindung mit der Rechtsabteilung) am ehesten in der Lage, Mitarbeiter, die gegen die in der Organisation geltenden Sicherheitsregeln verstoßen, zur Verantwortung zu ziehen und zu sanktionieren. Dazu muss sie sich an der Erstellung und Aktualisierung dieser Regeln beteiligen und gleichzeitig sicherstellen, dass sie den Mitarbeitern regelmäßig zur Kenntnis gebracht werden.

In einer idealen Welt wären alle Mitarbeiter eines Unternehmens für die Cybersicherheit verantwortlich und qualifiziert. Wenn dies der Fall wäre, **könnte das Unternehmen ihnen dann volles Vertrauen entgegenbringen?** Für Sébastien Viou *„schließt das Vertrauen nicht die Kontrolle aus. Sie könnte auf deren guten Glauben vertrauen, aber nicht auf deren Unfehlbarkeit. Selbst wenn sie sich alle an die Regeln der digitalen Hygiene halten würden, gäbe es kein Nullrisiko. Der vorsichtigste Mensch, manchmal sogar ein Experte für Cybersicherheit, kann darauf hereinfallen*". Diese Analyse wird durch den Aufschwung des Cloud-Computing oder Organisationsformen mit Telearbeit oder BYOD noch verstärkt. In diesem Zusammenhang können Unternehmen nicht mehr davon ausgehen, dass alles, was innerhalb ihres IT-Perimeters existiert, absolut vertrauenswürdig ist. Und immer mehr von ihnen übernehmen das Konzept „Zero Trust". Laut einer von IT SOCIAL veröffentlichten Studie beschäftigen sich 90 % der befragten Unternehmen ernsthaft mit diesem ganzheitlichen Ansatz, der darauf abzielt, das Konzept des Perimeters weiterzuentwickeln, indem niemandem innerhalb oder außerhalb des Unternehmensnetzwerks standardmäßig Vertrauen entgegengebracht wird. Für Joseph Graceffa ist Zero Trust jedoch *„nicht mehr und nicht weniger als ein weiterer Marketingbegriff*". Der Vorsitzende von CLUSIR Nordfrankreich erinnert daran, dass der Begriff zwar immer häufiger verwendet wird, es sich dabei aber vor allem um eine *„Aktualisierung der Verfahren der Network Access Control [NAC] handelt, die nun auf alle IT-Ressourcen (Anwendungen, Computerarbeitsplätze usw.) angewendet werden. Aber die CISOs und Spezialisten für Cybersicherheit kennen sie seit über 20 Jahren*". In jedem Fall ist die breite Anwendung eines Zero-Trust-Ansatzes eine Transformation, die extrem langwierig sein könnte, insbesondere für Unternehmen, die mit einem veralteten und abgeschotteten IT-Bestand arbeiten. Die Umsetzung dieses Ansatzes scheint daher schrittweise erfolgen zu müssen.

Cybersicherheit ist also nicht nur eine Frage der Mittel. Angesichts der Zunahme von Cyberangriffen besteht kein Zweifel mehr daran, dass der Mensch der größte Risikofaktor ist. Es ist daher von entscheidender Bedeutung, dass das Unternehmen seine Mitarbeiter ausbildet, sensibilisiert und schließlich in die Verantwortung nimmt. Denn wenn das Unternehmen Verantwortung für die Mitarbeiter übernimmt, übernehmen die Mitarbeiter Verantwortung für das Unternehmen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**

Version 1.1 - Copyright Stormshield 2022