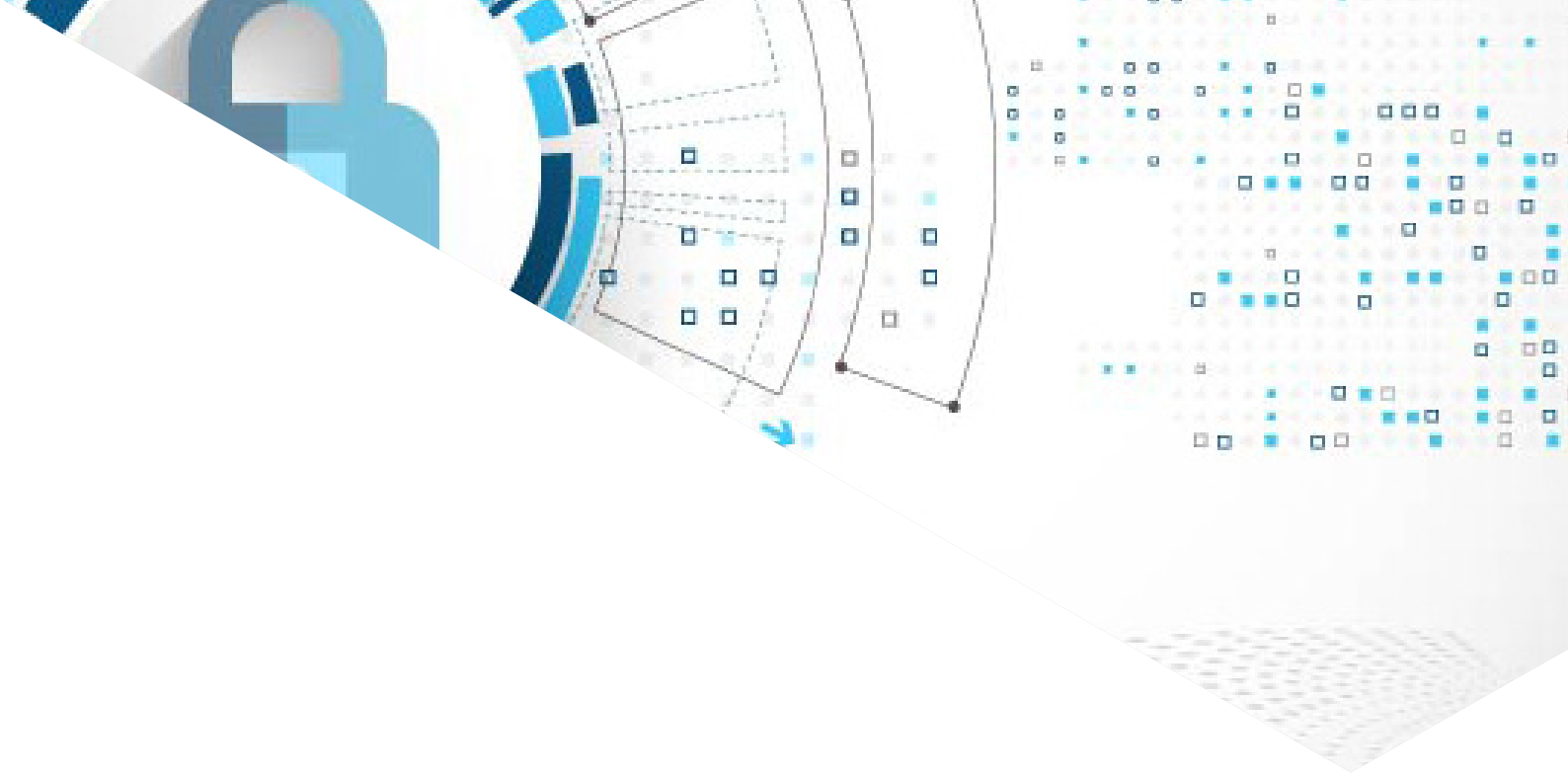


Cybersecurity und Risk Management für die Human Resources Abteilung

Cyber-Kriminalität – ein Begriff, der auch deutsche Unternehmen zunehmend unter Druck setzt: Laut einer Erhebung des Bundesamts für Sicherheit in der Informationstechnik (BSI) waren rund 70% der befragten Unternehmen im Jahr 2016/2017 Ziel von Cyber-Angriffen. Knapp die Hälfte der erfolgten Attacken konnten nicht ausreichend abgewehrt werden und verursachte messbare Schäden. Dabei gestaltet sich die Problematik weitaus komplexer als auf den ersten Blick angenommen: So ergab eine Untersuchung von Crowdresearchpartners, dass Sicherheitsexperten die eigenen Mitarbeiter im Unternehmen als einen der größten Risikofaktoren betrachten.

Auch in Zukunft ist kein Ende absehbar:

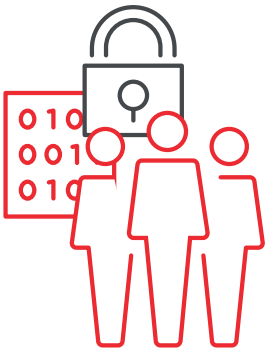
Nach einer Schätzung von Cybersecurity Ventures wird sich der durch Cyber-Kriminalität verursachte jährliche Schaden ab dem Jahr 2021 auf rund 6 Billionen USD belaufen.

6 Billionen USD ist die geschätzte jährliche Schadenssumme bis 2021

AON
Empower Results®

Risikoquelle Datenaustausch

Die Digitalisierung schreitet mit großen Schritten voran und hat bereits heute einen beträchtlichen Einfluss auf wirtschaftliche Abläufe: Denn der regelmäßige und stete Austausch von Daten ist wesentlich für den **Erfolg vieler Unternehmen** und kennzeichnet eine Entwicklung, die sich auch in den kommenden Jahren weiter fortsetzen wird.



Doch neben den ökonomischen Vorteilen des schnellen und unkomplizierten Austauschs findet sich hier auch der optimale **Nährboden für kriminelle Aktivitäten** mit dem Ziel, den **Geschäftsbetrieb zu stören** oder Assets in Form von **Aktiva oder** Geschäftsgeheimnissen abzugreifen. Um einen reibungslosen Daten- und Informationsaustausch über den gesamten Weg zu gewährleisten, sind Unternehmen deshalb heute mehr denn je auf den Einsatz und die Kompetenz **hochausgebildeter und spezialisierter IT-Mitarbeiter** angewiesen.

Human Resources als Business Partner der Cybersecurity

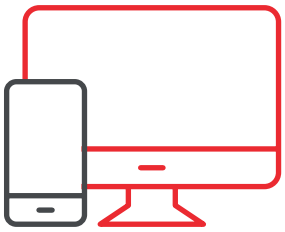
Die wichtigste Voraussetzung, um Cyberkriminalität angemessen begegnen zu können, liegt in der Gewinnung und langfristigen Bindung der richtigen Mitarbeiter. Hier wird dem Bereich Human Resources eine wesentliche Rolle zuteil: Als Business Partner für den IT-Bereich bringt er das notwendige Know-how in Sachen Suche und Vergütung spezialisierter Cybersecurity-Experten mit und sorgt dafür, dass wichtige Schlüsselpositionen innerhalb kurzer Zeit bestmöglich besetzt werden.

Wichtig für HR: Ein gutes Verständnis der Cybersecurity-Funktionen
Mit welchen Themen beschäftigt sich ein Cybersecurity-Architekt, welche Herausforderungen meistert ein Vulnerability Tester – und inwiefern unterscheiden sich die beiden hinsichtlich ihrer Gehaltsvorstellung und der letztendlichen Vergütung? Wie bemisst sich der Wert der einzelnen Profile, und wie lassen sich die jeweiligen Funktionen in die gesamte Jobarchitektur einbetten? Das sind nur einige der Fragen, auf die Human Resources eine Antwort haben sollte. Denn ein tiefgreifendes Verständnis rund um das Thema Cybersecurity ist für einen kompetenten HR Business Partner und Rewards-Experten unabdingbar.

Doch nicht nur in Sachen Vergütung, auch im Hinblick auf die Mitarbeiterbindung ist das Know-how des HR Business Partners gefragt: Ein guter Cybersecurity-Architekt verfügt über ein tiefes Verständnis der Sicherheitsarchitektur und ist damit ein wertvolles Asset, das man langfristig im Unternehmen halten und nicht, z.B. aus Kostengründen, aufs Spiel setzen sollte.

Interne Risikopotenziale erkennen und vermeiden

Hohe Cyber-Risiken entstehen jedoch nicht immer nur durch Angriffe von außen: Auch interne Prozesse, unachtsame Handlungen der eigenen Mitarbeiter oder falsche Entscheidungen können die Sicherheit im Unternehmen gefährden. HR kann hier einen entscheidenden Beitrag leisten, um u.a. die folgenden Risiken einzudämmen:



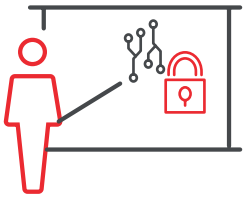
Fehleinschätzungen durch Online-Profile potenzieller Mitarbeiter

Erfolgreiche Projekte, beeindruckende Qualifikationen: Die online verfügbaren Informationen eines Mitarbeiters sind bereits heute oft wichtiger als sein Lebenslauf. Das Problem: Die auf professionellen Plattformen und Netzwerken eingestellten Inhalte sind meist nicht einwandfrei verifizierbar. Hier ist HR gefragt, das Profil eines Bewerbers anhand weiterer Quellen zu überprüfen und Inhalte kritisch zu hinterfragen – insbesondere bei verantwortungsvollen Senior-Positionen, die bei falscher Besetzung ein massives Reputationsrisiko darstellen.

Social Engineering Attacken

Der Begriff Social Engineering beschreibt die Manipulation oder Erpressung eines Mitarbeiters, um an wichtige Informationen zu gelangen. Die Gründe liegen auf der Hand: Auf diesem Weg erhalten Angreifer Zugänge zu Netzwerken oder geheimen Informationen oftmals schneller als durch komplexe technische Attacken. Durch intensives und strukturiertes Screening der Mitarbeiter kann HR an dieser Stelle dazu beitragen, Angriffe zu verhindern und das Risiko des Social Engineering zu mindern.

Unbedarfte Veröffentlichungen von Informationen



Das Bewusstsein rund um Cybersecurity schärfen und Verhaltensweisen der Mitarbeiter zielgerichtet schulen: Auch hier ist der Einsatz von HR gefragt, um die Gefahren der Cyber-Kriminalität weitgehend zu bannen. Denn auch das ausgefeilteste Access-Security-System kann für Unternehmen wertlos sein, wenn Mitarbeiter beabsichtigt oder unbeabsichtigt Informationen über ihren Arbeitgeber im Netz verbreiten. Mit durchdachten Maßnahmen versteht HR es auch an dieser Stelle, Risiken erfolgreich zu minimieren.

Reputations-Schäden durch Online-Identitäten

Einige Menschen besitzen online eine „zweite Identität“, die nicht mit der Firmenkultur vereinbar ist und deren Aufdeckung zu einem massiven Reputationsschaden des Unternehmens führen kann – ein Risiko, das sich mit zunehmender Seniorität einer Funktion im Unternehmen deutlich potenziert. Mit der Einführung und Überwachung einer soliden Social Media Policy kann HR hier optimale Rahmenbedingungen schaffen, um möglichen Schäden vorzubeugen.

Eine wachsende Herausforderung – auch für HR

In den kommenden Jahren wird die Thematik der Cybersecurity weiter an Bedeutung gewinnen. Doch schon heute stehen Unternehmen vor der Herausforderung, sich angemessen vor Angriffen zu schützen – eine Aufgabe, die das Unternehmen in seiner Gesamtheit angehen und nicht allein dem Cybersecurity-Team überlassen sollte.

Dabei ist auch der Einsatz von HR gefragt: Ein gutes Gesamtverständnis der einzelnen Cybersecurity-Funktionen und internen Risikopotenziale gepaart mit dem Anspruch, die Motivation der Mitarbeiter zu verstehen und sie nachhaltig zu begleiten – so kann Human Resources an vorderster Front sowohl direkt als auch indirekt eine wichtige Schlüsselrolle im gesamten Prozess einnehmen und einen wesentlichen Beitrag zu einer sicheren Unternehmensumgebung leisten.

Contacts

Ian D. Karcher
Leader – Central Europe Aon Rewards Solutions
+49 176 1266 4870
ian.karcher@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit: **http://aon.mediaroom.com**.

Empower Results®