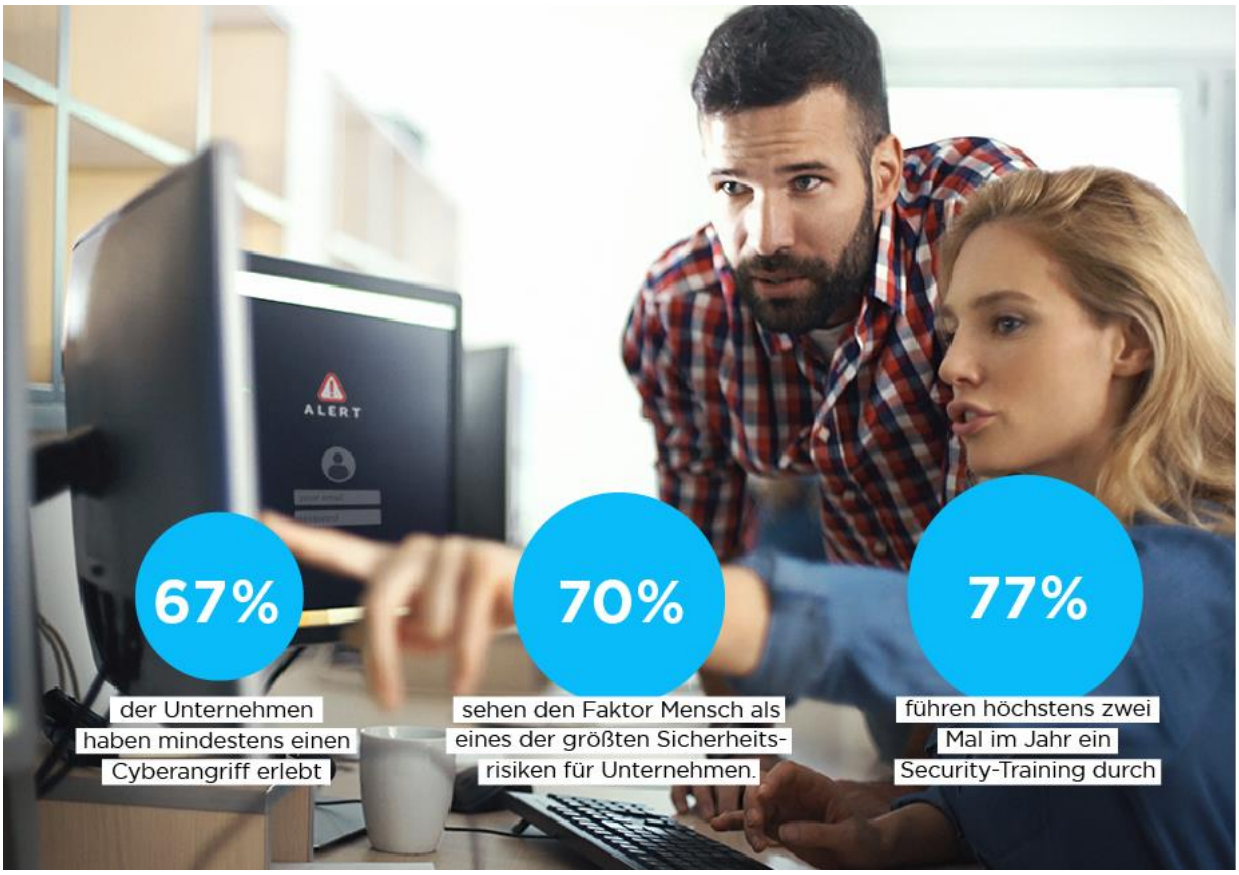
Cybersecurity Awareness-Experten: Vorboten der verborgenen Vorteile der Cybersicherheit

Geschrieben von Joshua Bucheli, KI-Ethik Forscher und Fellow at the ForHumanity Center, in Zusammenarbeit mit Sascha Maier, Head of IT und Cyber Resilience bei IWC Schaffhausen und Peter Kosel, Gründer von cyberunity



In der Unternehmenswelt ist die Digitalisierung so ziemlich allgegenwärtig. Sie ist nicht nur als lohnende Investition anerkannt, sondern bietet auch ein äusserst spannendes und praktisch endloses unternehmerisches Potenzial. Cybersecurity hingegen hat einen weitaus weniger beneidenswerten Ruf in den Unternehmen. Viele sehen darin nichts weiter als die unangenehme "Kehrseite der Medaille" der digitalen Innovation.

Wie der Volksmund sagt: Gibt dir das Leben Zitronen, mach Limonade und verkaufe sie mit Gewinn! Immer dann, wenn ein neuer Paradigmenwechsel neue Kosten mit sich bringt, sind diejenigen erfolgreich, die Wege finden, diese Kosten in Chancen umzuwandeln – so auch beim Thema Cybersicherheit.

Für Unternehmen bedeutet dies, dass sie Cybersecurity nicht mehr als eine Belastung sehen sollten, sondern als eine Investition – eine langfristige Chance, die mit der richtigen Aufmerksamkeit zu beträchtlichen Erträgen führen kann.

Wo steht das Thema Cybersecurity-Awareness heute?

«Seit dem Ausbruch der Pandemie hat die Idee, der Cybersicherheit Aufmerksamkeit zu schenken, an Zugkraft gewonnen. Dennoch tun sich die meisten Unternehmen immer noch schwer damit, die kulturellen Vorteile zu erkennen, welche die Awareness für Cybersecurity mit sich bringen kann», sagt Sascha Maier, Head of IT und Cyber Resilience bei IWC Schaffhausen.

Viele Unternehmen hinken der beängstigenden Geschwindigkeit, mit der sich neue Cyber-Bedrohungen entwickeln, noch immer hinterher. Führungskräfte gehen zu zaghaft an das Thema Sicherheit heran – sie implementieren bruchstückhafte Sicherheitslösungen, die auf einzelne Probleme abzielen, und meistens erst dann wenn sie entstehen:

«Zu viele gehen das Thema immer noch mit einer 'Erledigen statt Erreichen' -Mentalität an – sie verordnen gelegentliche E-Learnings und führen sporadische Phishing-Tests durch, weil sie es müssen, und nicht aus einem aufrichtigen Engagement für die Sicherheit heraus.»

Laut Sascha ist die Lösung dieses Problems "Awareness" mit einem grossen ‘A’:

«Unternehmen müssen erkennen, dass sie sich und ihre Stakeholder nicht nur besser schützen, sondern auch davon profitieren können, wenn sie das Thema Cybersicherheit ernst nehmen und es in ihre Unternehmenskultur und ihre Vermarktungsstrategien integrieren. Stattdessen steckt das Security-Bewusstsein der Unternehmen noch in den Kinderschuhen.»

Wohin bewegt sich das Thema Cybersecurity-Awareness?

Wie SANS OUCH! und ähnliche Publikationen zeigen, hat das Konzept der Cybersecurity Awareness die Bühne betreten. Jetzt muss es nur noch zum Leben erweckt werden und sich vom Komparsen zu einem der Hauptdarsteller entwickeln.

Wirksame Awareness ist allgegenwärtig und beinhaltet proaktive Sicherheitsschulungen, sorgfältige Nachbereitung von Sicherheitsverstössen und die Erkenntnis, dass ein solches Engagement für Cybersicherheit zu einem wertvollen Unternehmens-Image führen kann. Dazu berücksichtigt eine gute Awareness Kampagne auch die Kultur ihrer Zielgruppe, unabhängig davon, ob es sich dabei um eine bestimmte Abteilung oder das Unternehmen als Ganzes handelt.

«Wer 'Awareness' ernst nehmen will, muss es auch *leben*, sonst verpufft der Nutzen von Cybersecurity-Ausgaben ziemlich schnell», warnt Sascha.

Als Heimat des weltberühmten Crypto Valley und dank der internationalen Anerkennung ihrer vorausschauenden, innovationsfreundlichen Regulierungen ist die Schweiz ein perfektes Beispiel dafür, wie ein guter Ruf für Cybersicherheit Investitionen, Innovationen und andere

Chancen mit sich bringen kann. Dazu ist die Schweiz auch einer der vielversprechendsten Orte, wenn es um Karrieren in der Cybersicherheit geht.

«Die meisten Grosskonzerne sind bereits auf einem guten Weg, das wahre Potenzial der Cybersecurity für ihren Unternehmenserfolg zu nutzen. KMUs hingegen haben noch immensen Nachholbedarf», beobachtet Sascha.

Alle bereiche eines Unternehmens müssen sich einbringen und einen partizipativen und innovativen Ansatz verfolgen, der Cybersecurity in einem spannenden, positiven Licht erscheinen lässt. Persönlichkeiten, die diesen Wandel katalysieren können, indem sie ansprechende Tools nutzen, um die Awareness für Cybersecurity zu erhöhen und das Branding zu verbessern, sind daher absolut unerlässlich. Gute Methoden um eine Awareness Kampagne zu planen sind Lego Serious Play, das Framework von Spiral Dynamics Integral, oder das Security Awareness Planning Kit von SANS.

Cybersecurity Awareness-Spezialisten: Gefragte Fähigkeiten und Ausbildungen

Wollen Sie als externer Berater zukunftsorientierte Unternehmen beim Aufbau ihrer Unternehmenskultur unterstützen? Oder sind Sie eher daran interessiert, Teil der sprichwörtlichen "Speerspitze" zu werden, indem Sie sich Unternehmen anschliessen, die bereits an der Front dieses Paradigmenwechsels stehen? An Möglichkeiten mangelt es nicht.

Unabhängig davon, welchen Weg Sie einschlagen, werden bestimmte Fähigkeiten und Kompetenzen entscheidend sein:

Wenn es um Qualifikationen geht, sind die üblichen Zertifikate wie CISSP-, CISA- und CISM-Zertifizierungen zwar erwähnenswert, aber nicht so wichtig wie in anderen Bereichen der Cybersecurity.

Viel wichtiger sind der Nachweis eines soliden Verständnisses der menschlichen Risiken für die Informationssicherheit und wie man ihnen begegnet, professionelle Abschlüsse wie ICT Security Expert ED und Cyber Security Specialist EFA, nachgewiesene Kenntnisse der Branchen-Compliance-Standards und eine Weiterbildung in IUS.

Digicomp bietet auch einen guten Startpunkt, den Sascha für diejenigen sehr empfiehlt, die einen Einblick in die grundlegenden Tools einer Sensibilisierungskampagne erhalten möchten.

Personality: über technisches Know-How hinaus

Neben technischem Know-How sind ausgeprägte soziale und kommunikative Fähigkeiten unabdingbar für Cybersecurity-Awareness-Experten. «Die Verbesserung der Cybersecurity-Awareness ist mehr eine Frage der emotionalen Intelligenz als der technischen Expertise – es braucht Menschen, die eher psychologische Nuancen aufgreifen als technische Feinheiten. Aus diesem Grund werden reine Technophile nicht die Lösung sein», sagt Sascha.

Stattdessen werden sich Firmen zunehmend auf Mitarbeitende verlassen, die die Stakeholder davon überzeugen können, dass ein ehrliches Engagement für die Cybersicherheit wichtig ist. Es braucht Personen, die die Bedürfnisse aller Beteiligten, vom CEO über die Investoren bis hin zu den Produktionsmitarbeitern, erkennen und die das Thema Cybersicherheit in deren Kontext formulieren können.

Eng damit verbunden und wie in anderen Cybersecurity-Berufen ist auch hier bei Bewerbungen eine empathische Ader zu betonen. Die Fähigkeit, sich in andere hineinzuversetzen und die Dinge aus deren Perspektive zu sehen, ist entscheidend, um zu verstehen, wie man Informationen auf effektive Weise präsentiert.

Was Unternehmen vor allem brauchen, sind Spezialisten, die in der Lage sind, Denkweisen zu verändern, Probleme neu zu formulieren und das zukünftige Image der Cybersicherheit zu definieren, sowohl branchenübergreifend als auch innerhalb einzelner Unternehmenskulturen.

Das bedeutet Personen, die in der Lage sind, Awareness-Kampagnen zu entwerfen, durchzuführen und deren Wirksamkeit zu reflektieren – Individuen, die Fokusgruppen mit relevanten Stakeholdern aus allen Unternehmenshierarchien zusammenstellen können, um Cybersecurity-Bedenken so umfassend und proaktiv wie möglich zu identifizieren und anzugehen. Also Menschen mit einem Hintergrund in Marketing, Unternehmenskommunikation und Journalismus, Kreative aus R&D-Abteilungen und sogar Leute mit Erfahrung im Personalwesen.

Letztendlich sind es Marketing-Fähigkeiten, kreatives, unkonventionelles Problemlösungspotenzial, eine Leidenschaft für Cybersicherheit und ein Händchen dafür, Menschen zu begeistern und einzubeziehen, die das Profil eines starken Cybersecurity Awareness-Experten abrunden.

Wie Peter Kosel, Gründer, Talent Community Manager und Pionier des KNOW YOUR TALENTS Rekrutierungsansatzes bei cyberunity abschliessend feststellt:

«Cybersecurity Awareness ist ein Thema, bei dem die interdisziplinäre Zusammenarbeit im Vordergrund steht. Wer Cybersecurity im Unternehmen als lästiges Übel oder als reines Compliance-Thema betrachtet, erzielt weder Sicherheit noch einen wertvollen kulturellen Nutzen. Haltung entscheidet! Cybersecurity Awareness und damit verbundene Weiterbildungen wie das Leadership-Seminar von Digicomp sind wertvolle Möglichkeiten für Arbeitgeber, ihre Mitarbeitenden besser kennenzulernen und gemeinsam mit ihnen eine durchdringende Unternehmenskultur der Sicherheit zum Nutzen aller aufzubauen – denn Cybersecurity heisst KNOW YOUR PEOPLE.»