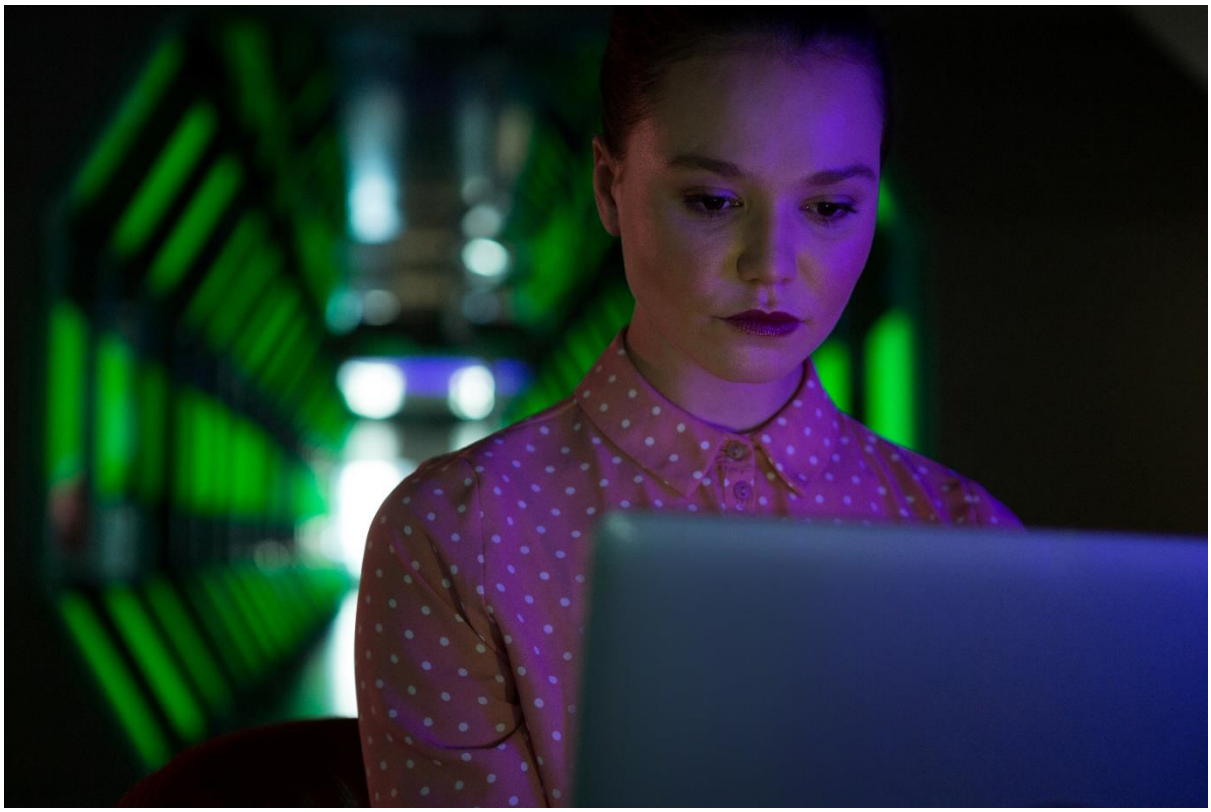
Führungspersönlichkeiten in der Informationssicherheit: Wegbereiter für ein umfassendes Sicherheitsmanagement

Geschrieben von Joshua Bucheli, KI Ethik Forscher und Fellow beim ForHumanity Center, in Zusammenarbeit mit Dr. Doron Zimmermann, Chief Cyber Security Officer, und Peter Kosel, Gründer von cyberunity



Um ein Unternehmen erfolgreich zu führen, ist es wichtig, die richtigen Prioritäten zu setzen und die richtigen Persönlichkeiten zu mobilisieren, die diese umsetzen. Während diese Prioritäten je nach Branche stark variieren können, bleibt die eine allgegenwärtig und wird dennoch unterschätzt – die Sicherheit.

Das Thema Unternehmens- und Cybersicherheit wird oft mit einer Art stillem Krieg verglichen, der um uns herum tobt, ohne dass die meisten von uns es überhaupt bemerken – ein Kampf zwischen denen, die unsere digitalen Werte schützen, und denen, die sie ausnutzen wollen.

Obwohl dies klischeehaft ist, lässt sich aus dieser kämpferischen Analogie für die Cybersicherheit etwas ableiten:

So wie eine effektive Armee sowohl aus gut ausgebildeten Soldaten als auch aus scharfsinnigen Generälen besteht, kommt es bei effektiver Cybersicherheit im Unternehmen sowohl auf fähige Spezialisten als auch auf kluge Führungspersönlichkeit an.

Ein Unternehmen kann über so viele Kryptographen, Cloud-Sicherheitsspezialisten, Phishing-Experten, Sicherheitsscouts und Awareness-Spezialisten verfügen, wie es will. Wenn diese Mitarbeitenden nicht frühzeitig erkannt, eingestellt, koordiniert und proaktiv von umsichtigen Führungskräften eingesetzt werden, die die Sicherheitsbedürfnisse wirklich verstehen und einzuschätzen wissen, wird ihr Potenzial weitgehend verpuffen.

Wo steht das Thema Corporate Security Heute?

Nach Maslows bekannter Bedürfnispyramide rangiert Sicherheit in der Hierarchie der menschlichen Ansprüche an zweiter Stelle nach den physiologischen Faktoren. Was aber immer noch zu oft übersehen wird ist, dass dies auch für Unternehmen gültig ist.

Nach wie vor werden die Vorteile zu wenig wahrgenommen, die aus einer integralen Sicherheitsstrategie folgen, obwohl diese im Sinne der Qualitätssicherung die Grundlage von nachhaltigen Beziehungen zu den eigenen Mitarbeitenden und Kunden darstellt. Hier sind in erster Instanz die Verwaltungsräte mit Ihrem Führungsgremium gefragt, um die Relevanz und den Anspruch an Sicherheit ihres Unternehmens zu definieren, zu konzipieren und schliesslich in die Umsetzung zu bringen.

Eine weitere wichtige Dimension für die Umsetzung der Sicherheitsstrategie liegt in der Gewinnung der richtigen Spezialisten und Persönlichkeiten, die diesem anspruchsvollen und zukunftsgerichteten Thema Leben einhauchen. Werden die Fühler erst dann ausgestreckt, wenn die Notwendigkeit an zusätzlicher Expertise erkannt wurde ist es viel zu spät wie Peter Kosel, Gründer der cyberunity AG herausstellt. Moderne Personalgewinnung ist mindestens eine, eher zwei Nasenlänge voraus und bereits mit den zukünftigen Mitarbeitenden in Kontakt bevor eine Vakanz entsteht. Die Devise heisst KNOW YOUR TALENTS statt WAR FOR TALENTS.

Oftmals konzentrieren sich Planungen zur Unternehmenssicherheit zu sehr auf die kleinteiligen, operativen Dimensionen und sagen wenig darüber aus, wie die Sicherheit von Führungskräften und Spezialisten gesamthaft angegangen werden sollte.

Unternehmen neigen noch zu oft dazu, die Risiken herunter zu spielen und verweisen auf die erheblichen Kosten, die mit umfassenden Sicherheitsstrategien verbunden sind. Doch das ist ein Fehler - die Bilanz wird durch einen laxen Umgang mit Sicherheit weit mehr gefährdet als durch die Investitionen, die sie erfordert – ganz zu schweigen von den unzähligen verborgenen Vorteilen, die Sicherheit einem Unternehmen bringen kann.

«Das Thema Sicherheit wird noch in zu vielen Unternehmen als ein peripherer Support-Prozess mit niedriger Priorität betrachtet, obwohl es sich in Wirklichkeit um einen grundlegenden Managementprozess handelt, der sorgfältige Investitionen in nachhaltige Beziehungen mit Kunden und Stakeholdern erfordert. Integraler Unternehmensschutz ist die Grundlage für das Überleben eines jeden Unternehmens, unabhängig davon, ob sich die Unternehmensleitung dessen bewusst ist», sagt Dr. Doron Zimmerman, Chief Cyber Security Officer.

Wohin bewegt sich das Thema Corporate Security?

Wie Doron betont, werden Führungskräfte immer mehr in Sicherheitsdiskussionen mit einbezogen. Dazu beginnen Unternehmen auch, Sicherheit durch die Linse von Risiken und Bedrohungen zu betrachten, statt nur als Nebenbeschäftigung der IT-Abteilung:

«Zu analysieren, welche Gefahren bestehen, zu bestimmen welche davon relevant sind, und sie dann entsprechend zu priorisieren, wird zunehmend zu einem Standardthema der Verantwortlichkeiten auf Managementebene. Diese Gefährdungen in Bezug auf die Stärken und Schwächen des jeweiligen Unternehmens zu betrachten, ist ebenfalls eine erfreuliche Entwicklung.»

Auch wenn der Umfang solcher Praktiken begrenzt ist, so sind sie doch ein Schritt in die richtige Richtung, wenn es darum geht, die Unternehmensleitung in das Thema Sicherheit einzubeziehen. Nur ein echtes Engagement der Führungskräfte für die Sicherheit und eine

ehrliche Betrachtung der Risiken wird es den Unternehmen ermöglichen, mit den sich ständig weiterentwickelnden Bedrohungen der digitalen Welt annähernd Schritt zu halten.

Unternehmen sind darauf fokussiert, eine stabile Umgebung zu gewährleisten, in der sie ihre Geschäfte abwickeln können:

«sie wollen sicherstellen, dass ihre Produkte, Dienstleistungen und Lösungen so sicher sind, dass sie ihre Kunden halten und neue Kunden gewinnen können. Darüber hinaus sollte es im Interesse eines jeden seriösen Unternehmers liegen, die Arbeitsplätze seiner Mitarbeitenden durch entsprechende Sicherheitsvorkehrungen so zu gestalten, dass sie sich auch in Zukunft auf einen sicheren Arbeitsplatz verlassen können. Wird beispielsweise ein Unternehmen durch einen Cyberangriff vollständig stillgelegt, dann ist je nach Dauer das Betriebsausfalls auch der Fortbestand des Unternehmens bedroht», so Doron.

Um dies zu gewährleisten führt an einem umfassenden Sicherheitskonzept nichts vorbei. Wirksame Sicherheit muss auf breiter Basis konzipiert und aktiv geführt werden. Führungskräfte und Manager müssen eine klare Vision davon haben, was ein Unternehmen mit Hilfe der Sicherheit erreichen möchte, bevor sie sich der operativen Seite zuwenden und Spezialisten hinzuziehen.

Information Security Leaders – Gefragte Fähigkeiten und Ausbildungen

Da umfassende und innovative Sicherheit ein so grundlegender Faktor für das Überleben und den Erfolg eines Unternehmens ist, werden Sicherheitsstrategen (CISOs), die dazu beitragen können, diese Realität im Ethos eines Unternehmens zu verinnerlichen, unverzichtbar sein. Sicherheit ist ein dynamisches Thema, und es ist wichtig, dass diese Persönlichkeiten in der Lage sind, die sich entwickelnden Bedürfnisse vorherzusehen und entsprechend proaktiv zu agieren.

Dennoch werden CISOs mit einem Abschluss in Cybersicherheit und den gängigen Zertifikaten wie CISSP, CISA, CISM etc. nicht ausreichen: «Es sind beeindruckende Titel und Qualifikationen, die jedoch kein Garant dafür sind, dass ein umfassendes Sicherheitsprimat verfolgt und gelebt wird» betont Doron. Zudem werden in der Praxis zu oft Sicherheitsverantwortliche mit ausgeprägtem IT-Hintergrund angestellt, um die dringenden Sicherheitslücken schnell fixen zu können, statt Sicherheitsstrategen, die das Gesamtbild sehen.

Wie hier mehrmals hervorgehoben wurde, wird das Thema Sicherheit oft zu operativ angegangen. Um das bisher zu kurz gekommene Thema Sicherheit schnell anzugehen, verbunden mit dem grossen Drang rasch erste Erfolge vorweisen zu wollen, werden sowohl vom Anspruch als auch Personell zu viele Kompromisse eingegangen. Zugegeben führt ein solches Vorgehen zu Resultaten und ist in der Praxis häufig anzutreffen, doch, es fehlt noch zu oft das langfristige Denken, das in der Informationssicherheit dringend erforderlich ist.

Solche Perspektiven kommen am besten aus dem Sicherheitsmanagement und der Politikgestaltung. Sogenannte ‘Defence Intellectuals’, die aus hochstrategischen Bereichen der Risikominderung kommen – von ehemaligen Strafverfolgungs- oder Militärangehörigen bis hin zu Fachleuten für auswärtige Angelegenheiten und Geheimdienstanalysten – können strategische und analytische Fähigkeiten in die Führungsteams von Unternehmen einbringen.

Neben einem allgemeinen Verständnis von Risiko- und Unternehmensmanagement müssen Fachleute, die dabei helfen wollen, die Weichen für die Unternehmenssicherheit zu stellen, in der Lage sein, Verfahren und Richtlinien zu erarbeiten, anwenderorientierte Schulungen

zu entwickeln, Audits und Bewertungen zu beaufsichtigen, Prioritäten zu setzen und begrenzte Ressourcen entsprechend innovativ einzusetzen.

Letztendlich müssen Sicherheitsverantwortliche in Unternehmen in der Lage sein, die Kluft zwischen IT und Management zu überbrücken. Zertifizierungen, die Cybersecurity- und Risikomanagement-Essentials kombinieren, wie CISSP, CRISC und vor allem CISM, verschaffen zukünftigen Führungskräften in dieser Hinsicht einen wertvollen Vorsprung.

Persönlichkeit – über technisches Know-How hinaus:

Eine ausgewogene künftige Sicherheitsbeauftragte bringt mehr mit als nur die bereits erwähnten Hard Skills und Zertifikate. Ebenso wichtig sind zwischenmenschliche Fähigkeiten und eine ehrliche Wertschätzung dafür, was auf dem Spiel steht.

Anpassungsfähigkeit, unkonventionelles Denken und die Fähigkeit, auch unter Druck einen kühlen Kopf zu bewahren, sind beispielhafte Schlüsselattribute für jeden, der sich mit der Bedrohungslandschaft der modernen Unternehmenssicherheit auseinandersetzen will. Ein starkes Netzwerk in der Security-Community verbunden mit einer Leidenschaft für Fragen der Sicherheitsführung, die durch die Teilnahme an Veranstaltungen wie der ASIS Europe Konferenz demonstriert wird, sind ebenfalls ein unbestreitbarer Vorteil.

Darüber hinaus ist ein Verständnis für die Bedeutung von Sicherheit und die Fähigkeit, sich für den notwendigen Wandel in der Branche einzusetzen, ebenfalls entscheidend. Oftmals konzentrieren sich Stellenbeschreibungen für Sicherheitsverantwortliche stark auf die operativen Dimensionen der Sicherheit. In solchen Fällen liegt es an den angehenden Führungskräften für Unternehmenssicherheit, die Notwendigkeit des Themas überzeugend darzustellen.

«Der Mensch ist die Quelle der Sicherheit, aber er ist auch die Quelle der Schwachstellen. In diesem Sinne ist Sicherheit ein 'People-Business' – eine soziale Angelegenheit», sagt Doron. In der Tat haben Studien gezeigt, dass 99% der Verletzungen der Datensicherheit auf menschliche Schwachstellen zurückzuführen sind.

In einer Welt, in der etwas so unscheinbares wie das Benutzen eines unbekannten USB-Sticks ein Unternehmen lahmlegen kann, ist die Verteidigung gegen immer häufiger auftretende Bedrohungen, die von Phishing-Angriffen und Ransomware bis hin zu ausgewachsenen Hacks reichen, vor allem eine Frage der Eindämmung von Insider-Bedrohungen. Dabei kommt es darauf an, sowohl mit den einzelnen Sicherheitsteams als auch mit den regulären Mitarbeitenden effektiv darüber zu kommunizieren, wie das Unternehmen am besten geschützt werden kann.

Alles in allem gibt es kein Patentrezept für einen effektiven Security Leader, und das hat viel mit der Tatsache zu tun, dass es sich um eine Funktion handelt, die sich noch weiter entwickeln wird. Sicher ist jedoch, dass gerade die Menschen, die diese Funktion ausfüllen, selbst die grösste Rolle bei der Definition dieser Position spielen werden.

Peter Kosel fasst zusammen dass eine strategische Verankerung des Themas Sicherheit in der Vision eines Unternehmens unerlässlich ist, um sowohl für Mitarbeitende, Kunden und die gesamte relevante Umwelt des Unternehmens das Grundbedürfnis nach Sicherheit zu befriedigen. Feuerlöscher aufhängen ist für den Notfall sinnvoll, doch was tun wir dafür, dass diese nicht zum Einsatz kommen?