Financial Times normiert Buchprojekt eines ehemaligen Informatik Studenten aus Reutlingen

20.04.2022, 14:52 | Wissenschaft, Forschung, Bildung

Pressemitteilung von: *Hochschule Reutlingen*
Presseagentur: *Hochschule Reutlingen*

Manuel Hepfner wird als Nachwuchsautor für das beste Business-Buchvorhaben des Jahres nominiert. Business Buch befasst sich mit Cyberangriffen im Netz.

Besondere Auszeichnung Dr. Manuel Hepfer. Die Financial Times in London normierte den Alumnus der Wirtschaftsinformatik Reutlingen für den Bracken Bower Preis 2021 . Am Ende zählte er sogar zu den drei Finalisten. Mit dem renomierten Preis zeichnet die Financial Times jährlich in London gemeinsam mit McKinsey einen Nachwuchsautor unter 35 Jahren für das beste Business-Buchvorhaben des Jahres aus, das überzeugend und unterhaltsam einen Einblick in zukünftige Trends in Wirtschaft, Finanzen oder Management bietet.

Manuel Hepfer studierte von 2011 bis 2015 Wirtschaftsinformatik an der Fakultät Informatik der Hochschule Reutlingen. Nach seinem Bachelor absolvierte er einen Master an der London School of Economics und promivierte anschließend an der University of Oxford. Heute ist der 30-jährige Doktor bei ISTARI-Global tätig, einem Unternehmen des singapurischen Staatsfonds, welches Organisationen dabei unterstützt Cyber-Resilienz aufzubauen. In seinem Buch geht Manuel Hepfer auf das Thema ein, dass ihn seit seiner Promotion und auch in seiner jetzigen Tätigkeit maßgeblich beschäftigt: Cyberattacken. Manuel Hepfer erzählt anhand persönlicher Anekdoten wie Vorstände und Manager mit schwerwiegenden Cyberangriffen umgehen und macht so das Thema zu einer spannenden Lektüre - nicht nur für IT-Experten.

Einen ersten Einblick in das Buch vermittelt das für den Bracken Bower Preis von Manuel Hepfer verfasste Exzerpt des Buches "The cybersecurity wake-up call: Building resilience in the digital age".

The cybersecurity wake-up call

Übersetzung des englischen Exzerpts, erschienen in der Financial Times

VON MANUEL HEPFER

"Diesen Moment werde ich nicht mehr vergessen. Es war früh am Morgen, als ich um 4 Uhr von einem Anruf geweckt wurde", sagte Robert Frazer, Vorsitzender des Aufsichtsrates eines großen internationalen Unternehmens. (Robert Frazer ist nicht sein richtiger Name). "Aus dem Büro kam ein Anruf, dass wir einen schweren Cyberangriff erlitten hätten, der unser Geschäft komplett zum Erliegen brachte. Wir mussten unsere gesamte IT-Infrastruktur neu installieren - mehr als 4.000 Server, 50.000 Laptops, 3.000 Applikationen."

Robert erzählte weiter: "Dieser Cyberangriff war ein richtiger Weckruf für ein globales Unternehmen wie uns - und auch ein sehr teurer. Dennoch behaupte ich, dass es ein sehr wichtiger Weckruf war. Ich hoffe, dass dieser Vorfall nicht nur für unser Unternehmen ein Weckruf war, sondern dass es einer für alle Unternehmen ist, die etwas mit Technologie zu tun haben. Ich nehme an, dass es sich dabei um jedes Unternehmen auf der Welt handelt."

Robert scheint eine Erfahrung mit einem außergewöhnlich schlimmen Cyberangriff zu schildern, allerdings war daran nichts außergewöhnlich. Immer wieder kommt es zu verheerenden Cyberangriffen.

The Economist beschreibt die aktuelle Lage der Cybersicherheit als Ransomware-Pandemie. Innerhalb von drei Wochen im Mai 2021 wurde die Welt Zeuge von drei hochkarätigen Cyberangriffen. Am 7. Mai griffen Cyberkriminelle den US-Pipelinebetreiber Colonial Pipeline an, eine Hauptleitung, welche fast die Hälfte des Öls an die US-Ostküste liefert. Die Cyberattacke führte zu Benzinknappheit und langen Warteschlangen an Tankstellen. Nur wenige Tage später, am 13. Mai, legte ein Cyberangriff viele Krankenhäuser in Irland lahm und verursachte so erhebliche Einschränkungen ambulanter Dienste. Zwei Wochen später, am 30. Mai, traf ein ähnlicher Cyberangriff den weltgrößten Fleischproduzenten, JBS Meat, und legte seine Rinder- und Schweineschlachthöfe lahm.

Die Bedrohung durch Cyberangriffe ist zu einem großen Risiko für die Rentabilität und den Geschäftserfolg von Unternehmen geworden. Laut einer Studie der London Business School hat sich das Risiko Ziel einer Cyberattacke zu werden seit 2013 verdreifacht. Das Weltwirtschaftsforum führt Cyber-Sicherheitsrisiken weiterhin als eines der gravierendsten Unternehmensrisiken. Was vor Jahrzehnten bloß ein Gesprächsthema unter Computer-Nerds war, ist heute eine der drängendsten organisatorischen und gesellschaftlichen Herausforderungen. In unserem digitalen Zeitalter ist die Gefahr durch Cyberangriffe größer denn je.

Unternehmen, die Opfer eines schweren Cyberangriffs geworden sind, verstehen, dass Cyberangriffe nicht verhindert werden können. Die Erkenntnis über unsere Unfähigkeit, Cyberangriffe vollständig zu verhindern, ist ernüchternd. Obwohl die Ausgaben für Cybersicherheit jedes Jahr steigen, treten schlimme Angriffe immer häufiger auf. Selbst die größten und technologisch fortschrittlichsten Unternehmen wie Apple, Google, Facebook, Yahoo, JPMorgan Chase oder sogar das US-Militär haben bereits unter Cyberangriffen gelitten. Wenn diese Unternehmen Cyberangriffe nicht vollständig verhindern können, wer soll es dann können? Die kurze Antwort lautet: Kein Unternehmen ist dazu in der Lage.

Darum müssen sich Unternehmen auf Cyberangriffe vorbereiten. Die meisten schwerwiegenden Cyberangriffe passieren nicht, weil ein Mitarbeiter auf einen schädlichen Link in einer Spam-E-Mail geklickt hat. Oft erfolgen sie, weil Angreifer Wochen damit verbringen, durch ganz normale Geschäftstransaktionen Wege in Unternehmensnetzwerke zu finden. Unternehmen haben häufig Schwierigkeiten, das Eindringen zu erkennen. Daher reicht es nicht aus, in Cybersicherheit zu investieren. Unternehmen sollten sich darüber hinaus auf die Stärkung ihrer Resilienz konzentrieren.

Cybersicherheit und Resilienz sind zwei verschiedene Konzepte. Ihre Unterschiede zu verstehen ist wichtig für Unternehmen, die im heutigen digitalen Zeitalter nicht nur überleben, sondern Erfolg haben wollen. Das Ziel von Cybersicherheit besteht darin, Cyberangriffe zu verhindern und somit die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten zu schützen. Resilienz dagegen ist die Fähigkeit einer Organisation, Cyberangriffe zu antizipieren, ihnen zu widerstehen, sich zu erholen und daraus zu lernen. Konkret bedeutet dies, Auswirkungen eines Angriffs zu minimieren und die organisatorische Leistungsfähigkeit möglichst schnell wiederherzustellen.

Was bei einem schweren Cyberangriff wirklich in Unternehmen passiert - und was sie daraus lernen - bleibt der Öffentlichkeit oft weitgehend verborgen. Als Forscher an der Universität Oxford erhielt ich Insider-Zugang zu Unternehmen, die von einem schweren Cyberangriff betroffen waren. Ich habe die Geschichten mehrerer Unternehmen

studiert, die Opfer nationalstaatlicher Spionage-Cyberangriffe und verschiedener Formen von Ransomware wurden. Ich habe Chief Executives, Chief Financial Officers, Chief Information Officers, Chief Information Security Officers, andere Führungskräfte und IT-Administratoren interviewt. Unter der Bedingung der Anonymität erhielt ich umfassenden Zugriff auf interne Dokumente, Präsentationen sowie Audio- und Videodateien zu Ereignissen vor, während und nach dem Cyberangriff. Ich habe die Daten systematisch analysiert und suchte nach Mustern, Gemeinsamkeiten und Unterschieden.

Dieses Buch hat zwei Ziele. Erstens soll es ein Weckruf für Cybersicherheit im digitalen Zeitalter sein. Um dies zu erreichen, teilt das Buch unveröffentlichte Insidergeschichten von Führungskräften, die ihr Unternehmen durch verheerende Cyberangriffe geführt haben - ihre Erfolge, Fehler, Lehren und Erkenntnisse für die Zukunft. Für viele Führungskräfte waren Investitionen in Cybersicherheit zuvor ein reiner Kostenfaktor und die Bedrohung durch Cyberangriffe ein operatives Risiko. Nachdem sie ihr Unternehmen durch einen schweren Angriff geführt hatten, verstanden sie Cyberangriffe als strategisches Risiko, das das Überleben ihres Unternehmens gefährden kann. Vor allem aber begannen sie, Cyber-Resilienz als strategische Chance im digitalen Zeitalter zu betrachten.

Zweitens zeigt dieses Buch, was wir gegen das wachsende Problem der Cyber-Bedrohungen tun können: eine Reorientierung von klassischer Cybersicherheit hin zur Stärkung organisatorischer Resilienz. Da Cyberangriffe nicht verhindert werden können, bietet das Buch The Cybersecurity Wake-Up Call einen praktischen Leitfaden zur Stärkung von Cyber-Resilienz.

Verantwortlicher für diese Pressemitteilung:

Hochschule Reutlingen
Herr Siewe-Reinke Alfred
Alteburgstraße 150
72762 Reutlingen
Deutschland

fon ..: 07121 271 4052
web ..: http://www.informatik-reutlingen.de
email : presse@informatik-reutlingen.de

Pressekontakt:

Hochschule Reutlingen
Herr Siewe-Reinke Alfred
Alteburgstraße 150
72762 Reutlingen

fon ..: 07121 271 4052
web ..: http://www.informatik-reutlingen.de
email : presse@informatik-reutlingen.de

News-ID: 1227824 • Views: 1100 (Stand: 30.04.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1227824/Financial-Times-normiert-Buchprojekt-eines-ehemaligen-Informatik-Studenten-aus-Reutlingen.html