fakten
Iskro Mollovs Freizeit gehört zu einem guten Teil seinen beiden kleinen Kindern im Alter von fünf und sieben Jahren. „Ich versuche so viel Zeit wie möglich mit ihnen zu verbringen", erzählt der 39-Jährige. Für das Sportstudio, das er früher mehrmals die Woche besuchte, bleibt **neben Familie und Job** dagegen nur noch selten Zeit.

Iskro Mollovs: Ein Thema für jede Unternehmensführung

großes interview
Iskro Mollov verantwortet beim Anlagenbauer GEA Group die **Informationssicherheit**. Im Interview erzählt er, wie er seine Arbeit organisiert.

Text: Armin Fuhrer
Foto: Presse/GEA Group

Herr Mollov, wie wichtig ist eine ausgereifte Strategie zur (Cyber-)Sicherheit?
Dass Unternehmen eine Strategie zur Abwehr von Sicherheitsrisiken inklusive Cyberattacken brauchen, steht außer Frage. Wir unterscheiden zwei Arten von Sicherheitsrisiken, auf denen unsere Sicherheitsstrategie aufbaut: zum ersten die operativen Risiken, also zum Beispiel, dass die Produktion oder die IT durch Verschlüsselung, Manipulation oder Sabotage stillgelegt wird oder Informationen abfließen. Und zum zweiten gibt es die Compliance-Sicherheitsrisiken. GEA ist in 62 Ländern aktiv und überall gibt es unterschiedliche Regeln und Gesetze sowie zahlreiche Anforderungen der unterschiedlichen Kunden. Dazu gehören auch mögliche Haftungsschäden, die man ausschließen muss.

Welches sind die größten technischen Gefahren?
Das ist schwer zu sagen, denn das größte Bedrohungspotenzial eines Unternehmens hängt von seiner Betätigung ab und davon, auf welchen Geschäftsfeldern es sich bewegt, und natürlich auch von seinen eigenen Schwachstellen. Das ist also von Fall zu Fall unterschiedlich. Ransomware ist eine sehr große Gefahr, denn wenn ein Unternehmen komplett verschlüsselt ist und möglicherweise nicht über Backups verfügt, dauert es lange, bis der Betrieb wiederhergestellt ist. Es ist nicht in erster Linie die Zahlung des geforderten Lösegeldes, sondern vielmehr die Betriebsunterbrechung, die zu einem sehr großen Problem wird. Die GEA Group zum Beispiel produziert hauptsächlich Anlagen für die Nahrungs- und Getränkeindustrie sowie Pharmaindustrie – da wäre ein längerer Ausfall der eigenen oder der Kundenproduktion sehr schlimm.

„Die Mitarbeiter sind immer noch eine der größten Schwachstellen, zum Beispiel, weil viele Angriffe über E-Mails starten."

Wie können sich Unternehmen gegen Cyberangriffe schützen?
Als ich Anfang 2020 bei der GEA Group anfing, habe ich mir als Erstes einen Überblick über die Ist-Situation verschafft. Das muss immer der erste Schritt sein. Auf dieser Analyse entwickelten wir dann eine Strategie, wie wir die Aufgaben, die sich daraus ergaben, im Unternehmen verteilen wollten. Wir erarbeiteten ein Dreijahres-Programm und acht strategische Workstreams, also Aufgabenfelder. Nach etwa zwei Jahren haben wir mehr als die Hälfte davon.

Wie organisieren Sie die Arbeit?
Um diese Frage zu beantworten, muss man zwei Dinge unterscheiden: unsere Programmorganisation, also die eben erwähnten acht Aufgabenfelder, und unsere Linienorganisation. Zum ersten Punkt: Für jeden Workstream habe ich einen oder mehrere Workstreamleads bestimmt, bei denen es sich in der Regel um die jeweiligen Leiter der Fachbereiche handelt. Sie arbeiten bei der Entwicklung der Sicherheitsstrategie mit und implementieren sie auch in ihre Bereiche. Diese Kollegen gehören zwar nicht zu meiner Abteilung, aber sie berichten mir fachlich in Sicherheitshinsicht. Für die Linienorganisation habe ich eine zentrale Abteilung mit etwa 25 Mitarbeitern. Hier arbeiten Experten mit Fachwissen in den unterschiedlichen Sicherheitsbereichen. Diese Mitarbeiter betreuen ihre Fachgebiete zentral. Zusätzlich gibt es Sicherheitsexperten in den Regionen und an den Standorten.

Muss das Thema Cybersicherheit in der Führung angesiedelt sein?
Informationssicherheit ist unbedingt ein sehr wichtiges Thema für jede Unternehmensführung. So ist auch bei der GEA Group, wo es ganz oben angesiedelt ist. Ich berichte quartalsweise dem Prüfungsausschuss des Aufsichtsrats und regelmäßig dem Vorstand.

Wie wichtig ist der Faktor Mensch mit Blick auf die Informationssicherheit?
Die Mitarbeiter sind immer noch eine der größten Schwachstellen, zum Beispiel, weil viele Angriffe über E-Mails starten. Daher sind regelmäßige Schulungen und Sensibilisierungsmaßnahmen notwendig. Bei uns ist jeder Mitarbeiter verpflichtet, immer an die Sicherheit zu denken. Wir haben zusätzlich eine ganze Reihe von Maßnahmen wie regelmäßige Awareness-Kampagnen. Am besten ist es aber, mit technischen Maßnahmen möglichst weitgehend zu vermeiden, dass es überhaupt zu menschlichen Fehlern kommt.

Stellt es ein Problem dar, dass Sie auf die Lieferketten und Zulieferer nicht so einen großen Einfluss haben wie auf das eigene Unternehmen?
Wir setzen gegenüber unseren Lieferanten unsere Policy durch und überprüfen sie, bevor wir mit ihnen anfangen zu arbeiten. Aber natürlich können wir nicht überprüfen, ob alle den Sicherheitsanforderungen auch wirklich nachkommen. Wir müssen ihren Nachweisen und Angaben zum großen Teil vertrauen, da wir nicht alle auditieren können. Ein Restrisiko besteht aber natürlich immer.

„Der härteste Tresor bringt nichts, wenn das Schloss aus Holz ist!"

Andreas Papadaniil,
CEO des It-Security Consulting-Unternehmens suresecure.

interview
Andreas Papadaniil spricht über **Herausforderungen und Chancen** der Cloud-Security.

Text: Jakob Bratsch, Foto: Presse/suresecure

Ihr Unternehmen setzt immer mehr auf Cloud-Security, wie blicken Sie auf den Cloud-Security-Markt?
Wir sehen einen steigenden Markt, der dynamisch ist und der sich täglich ändert. Studien schätzen, dass die Ausgaben für Cloud-Security jene der klassischen IT-Security in drei Jahren überholen werden. Aber für uns ist das eine große Chance. Wir haben bereits seit längerem damit begonnen Zertifikate zu erlangen, und Partnerschaften mit Cloud-Anbietern zu knüpfen.

Welche Herausforderungen müssen Sie bei der Beratung Ihrer Kunden dabei im Blick haben?
Wir stellen häufig fest, dass wohl eine falsche Vorstellung beim Thema Cloud existiert. Cloud scheint einfach – so ist es aber nicht. Viele Unternehmen hören nur, dass dies die Zukunft ist und kaufen häufig Cloud-Kapazitäten, die für ihr Business aber nicht sinnvoll sind. Und die Sicherheit in Bezug auf Cloud-Lösungen wird dabei auch häufig unterschätzt. Cloud ist die Zukunft und bietet bei richtiger Anwendung auch viele Möglichkeiten – aber eben auch neue Möglichkeiten für Cyber-Kriminelle. Es bringt Ihnen der härteste Tresor nichts – wenn das Schloss aus Holz ist.

Forschung für mehr Cybersicherheit

prävention

Cyberspezialistin Prof. Dr. Haya Shulman leistet mit ihren Forschungen einen wichtigen Beitrag für mehr **Sicherheit im Internet**. Ein Porträt.

Text: Julia Butz
Foto: Harald T. Schreiber, Bench Accounting/unsplash

Dr. Haya Shulman,
Leiterin der Abteilung Cybersecurity Analytics and Defences (CAD) am Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt und Leiterin des Forschungsbereichs Analytics Based Cybersecurity am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE

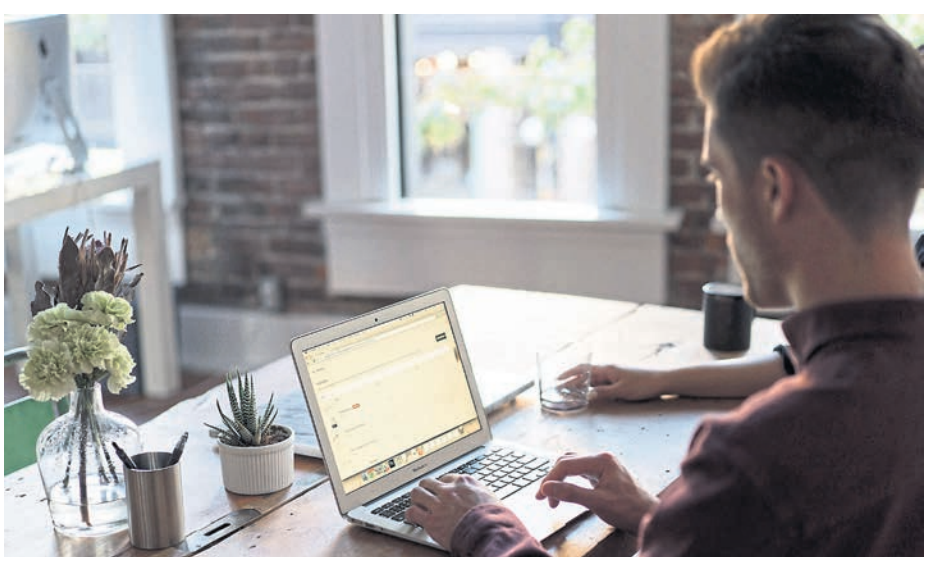
ATHENE begleitet die digitale Transformation aus Sicht der Cybersicherheit und des Privatsphärenschutzes. In einzelnen Forschungsbereichen werden Methoden und Technologien für Datensicherheit und Datenschutz für Organisationen und Verbraucher entwickelt. Dabei wird beispielsweise beobachtet, welche Schwachstellen in IT-Infrastrukturen einzelner Unternehmen, Universitäten, Behörden oder Parteien vorliegen, wie Sicherheitsmechanismen dort eingesetzt werden und für welche Angriffe die jeweiligen IT-Systeme empfänglich wären. Forschungsobjekt kann nicht nur eine bestimmte Organisation sein, sondern auch gesamte Wirtschaftssektoren oder Länder.

In den Forschungen von Dr. Haya Shulman geht es in den Grundsätzen immer darum, das Internet und seine Nutzung sicherer zu machen. Dabei wird auf praktischer Ebene erforscht, wie Angreifer vorgehen – um so zu ermitteln, wie verwundbar das Internet ist und daraus Rückschlüsse für die gezielte Entwicklung von Maßnahmen zur Vermeidung von Cyberangriffen ziehen zu können. Darüber hinaus beschäftigt sich Shulman und ihr Team damit, wie man die richtigen rechtlichen und wirtschaftlichen Anreize setzt, damit neue Sicherheitsverfahren in der Praxis auch eingesetzt werden. Im Rahmen ihrer Arbeit für die Entwicklung der Sicherheitslösung Cache-Test am Forschungszentrum ATHENE wurde Shulman 2021 mit dem Deutschen IT-Sicherheitspreis der Horst-Görtz-Stiftung ausgezeichnet.

In diesem Jahr ist Dr. Haya Shulman dem Ruf auf eine Professur am Institut für Informatik der Goethe-Universität Frankfurt gefolgt und hat dort eine LOEWE-Spitzen-Professur inne. Sie ist außerdem Gastprofessorin an der Hebräischen Universität Jerusalem in Israel sowie Initiatorin und Leiterin des Hessisch-Israelischen Partnership Accelerator Programms in Darmstadt und Jerusalem. Die Fachwelt zeichnete Shulman bereits 2015 mit dem Forschungspreis Applied Networking Research der Internet Research Task Force aus – der international wichtigsten Auszeichnung für herausragende Forschungsleistungen im Bereich der Internet-Technologien.

Haya Shulman ist überzeugt, dass die heute vorwiegend verwendeten Sicherheitsarchitekturen ausgedient haben und mehr für die digitale Sicherheit getan werden muss. Obwohl das Bewusstsein für die Gefahren durch Cyberangriffe in Deutschland hoch sei, blieben viele Organisationen hinter dem Stand der Technik zurück. Es bedürfe auch sehr viel mehr Vorbereitung für den Notfall, indem beispielsweise in moderne Ansätze wie Zero-Trust-Architekturen investiert würde. Zero-Trust gilt als eines der neuen Schlagwörter in der Cybersicherheit: eine Sicherheitsarchitektur, bei der jede Anwendung einzeln verschlüsselt ist und der Benutzer sich je Dienst vollständig authentifizieren und autorisieren muss. Das Prinzip der geringstmöglichen Zugriffsrechte trägt dazu bei, ein Netzwerk als Ganzes zu schützen, indem es Eindringlinge nicht über einen einzigen Zugang auf das gesamte System zugreifen lässt.

Cyberattacken abzuwehren hängt auch davon ab, wie gut ein Unternehmen vorbereitet ist. Wenn z. B. nach einem Ransomware-Angriff Unternehmens- und Infrastrukturdaten verloren sind, wird – sobald man den Angriff bemerkt, die gesamte IT heruntergefahren und auf ein Ersatzsystem neu aufgesetzt.



Es gilt, die Cybersicherheit an das wachsende Tempo der Digitalisierung anzupassen und Angreifern bestenfalls immer einen Schritt voraus zu sein.

Sind Back-ups vorhanden und wurde das Umschalten gut vorbereitet, können IT und Anwendungen innerhalb nur einiger Stunden oder weniger Tage hochgefahren werden und wieder laufen. Ausschlaggebend dafür ist eine gute Vorbereitung – und Übung. Also eine Art Cyber-„Brandschutz"-Übung, um für den Ernstfall vorzubeugen. Mit der Lernumgebung „Cyberrange" die die Forschenden in ATHENE aufgebaut haben, können derarte Abläufe unter realitätsnahen Bedingungen geübt werden.

Bei einer aktiven Cyberabwehr werden nicht nur potenzielle Angriffsziele minimiert, sondern angreifende Netze proaktiv blockiert oder auch Abwehrmechanismen eingesetzt, die die Infrastruktur des Angreifers nachhaltig beschädigen. Zu einer effektiven Cyberabwehr-Option gehört auch die Beseitigung von Schwachstellen im Netzwerk eines Unternehmens. Hier gilt es zu bestimmen, über welchen Weg die Angriffssoftware ihren Weg in das eigene Betriebsnetz gefunden hat und die zur Installation genutzte Schwachstelle zu schließen.

Dr. Shulman plädiert dafür, dass sich auch Unternehmen, die eigentlich nicht viel mit IT zu tun haben oder bislang hatten, mit der Thematik auseinandersetzen und aktiv handeln sollten. Denn alles, was vernetzt ist, kann prinzipiell auch angegriffen werden. Cyberkriminalität trifft nicht nur die Wirtschaft und kritische Infrastrukturen: Vereine, Parteien, Forschungseinrichtungen und Privatpersonen – sie alle stehen im Fokus von Cyberangreifern. Ob am Arbeitsplatz, im Smart Home oder am Computer zu Hause: Antivirus-Programme verwenden, Updates zulassen, regelmäßig Back-ups der eigenen Daten vornehmen und keine Dateien von unbekannten Quellen öffnen. Es gilt, die Cybersicherheit an das wachsende Tempo der Digitalisierung anzupassen und Angreifern bestenfalls immer einen Schritt voraus zu sein. Die Forschungsinitiativen für Cybersicherheit helfen dabei.

fakten

Laut Bitkom Research 2021 haben über 60 % der Unternehmen ihre Ausgaben für IT-Sicherheit zwar erhöht, gemessen am Gesamtbudget bleiben die Investitionen gering, da diese mit durchschnittlich nur 7 % zubuche schlagen. Aktuell haben 34 % ihre **IT-Schutzmaßnahmen kurzfristig hochgefahren**. (Bitkom-Umfrage 3/22)

„Mit einer 99 % Spam-Erkennungsrate gegen Cyberattacken"

Roger David,
Geschäftsführer windream GmbH

interview

Roger David über **Cybersicherheit**.

Text: Julia Butz
Foto: windream GmbH

Mit welchen Tools können sich Unternehmen vor Cyberattacken schützen?

Mailserver-Security-Software zum Schutz vor Spam-, Phishing- und Malware-Angriffen ist ein erster Schritt. Wir schützen Unternehmen durch unser Produkt eXpurgate, indem mit einer Spam-Erkennungsrate von über 99 % sichergestellt wird, dass nur wirklich businessrelevante Inhalte den Weg zum Empfänger finden. Auch gegen DDoS-Attacken wird eXpurgate erfolgreich eingesetzt.

Was raten Sie Ihren Kunden darüber hinaus?

Ganz wichtig sind vernünftige Back-ups und eine allumfassende Archivierung. So sind auch bei einer Verschlüsselungsattacke Dokumentarchive nicht veränderbar. Wir sind in der Lage, die Dokumentbestände mit allen Klassifizierungen, Merkmalen und Attributen vollständig wiederherzustellen. Dabei wird das Enterprise-Content-Management-system nahtlos an das ERP-System des Kunden gekoppelt, sodass er mit integrierten Systemen arbeiten kann.

Welche Rolle spielt der Faktor Mensch?

Die Sensibilisierung der Mitarbeiter und regelmäßige Schulungen sind immens wichtig. Vor allem in Zeiten von Mobile Offices, wenn Mitarbeiter für den privaten Computer einen Zugang zum Firmennetzwerk erhalten, ist das im Hinblick auf Cyberattacken und die kriminellen Unternehmen, die dahinterstecken, ein Riesenproblem. Ich sage bewusst Unternehmen, denn die Attacken gehen von absolut professionell agierenden Organisationen aus.

„Ganz wichtig sind vernünftige Back-ups und eine allumfassende Archivierung. So sind auch bei einer Verschlüsselungsattacke Dokumentarchive nicht veränderbar."