“Das Strafrecht schreckt nicht ab”

Expertengespräch zu IT-Compliance

(BS) Das Thema IT-Sicherheit ist inzwischen bei den Vorständen angekommen. Dies reicht jedoch nicht aus, um sich als Unternehmen oder als Behörde für Cyber-Attacken zu wappnen. Wichtig ist nicht zuletzt eine funktionierende IT-Compliance unter Einbeziehung aller Mitarbeiter. Im Interview mit dem Behörden Spiegel sprechen die IT-Experten Thomas Müller, Dr. Roderic Ortner, Dr. Carsten Wettich und Dr. Martin Wundram über IT-Compliance. Die Fragen stellte Tobias Henke.

V.l.n.r: Thomas Müller ist Geschäftsführer der DIE PR-BERATER GmbH mit Sitz in Köln, Dr. Roderic Ortner ist Fachanwalt für IT-Recht, Dr. Christian Wettich ist ebenfalls Rechtsanwalt und Dr. Martin Wundram arbeitet als IT-Forensiker für Gerichte und Staatsanwaltschaften. Fotos: BS/privat

Behörden Spiegel: *Herr Wundram, Welche Folgen kann ein Hacker-Angriff für Mitarbeiter oder den Betrieb eines Unternehmens haben?*

Wundram: Der Erfahrung der letzten Jahre nach sind Betroffene oft mit einem “blauen Auge” davongekommen. Zunehmend werden Angriffe von Tätern – egal ob Außentäter oder Innentäter – in ihren Auswirkungen jedoch schwerwiegender und letztlich auch teurer. Das Bekanntwerden auch intimer privater und dienstlicher Daten kann unangenehm, peinlich und im Extremfall existenzgefährdend werden.

Behörden Spiegel: *Der Datenhunger der Cyber-Kriminellen scheint immer größer zu werden.*

Wundram: So ist es. Bei dem Angriff auf Sony im Jahr 2014 haben die Täter angeblich 100 TeraByte Daten erbeutet und Teile davon auch veröffentlicht. Dies hat dem Ansehen des Unternehmens geschadet, insbesondere hat Sony zur Vorfallsbewältigung im ersten Quartal 2015 15 Millionen US-Dollar zurückgestellt. Auch persönliche Mitarbeiterdaten sind durch diesen Fall an die Öffentlichkeit geraten. Die 2015 angegriffene Datingplattform Ashley Madison wurde durch die Veröffentlichung der gesamten Kundendatenbank massiv erschüttert. Es werden sogar einige Suizide mit dem Bekanntwerden der pikanten Daten in Verbindung gebracht. Und dass konkrete Konfigurationsschwächen, gepaart mit “Datenbergen”, brandgefährlich und zugleich keine Seltenheit mehr sind, zeigt eindrucksvoll auch das Jahr 2016 mit “Panama Papers“ rund um den panamaischen Offshore-Dienstleister Mossack Fonseca.

Behörden Spiegel: *Welche Ziele verfolgen die Angreifer?*

Wundram: Da mittlerweile praktisch alles mit allem vernetzt ist, operieren Angreifer auch mit den unterschiedlichsten Motiven. Manche wollen wie *Snowden* Sachverhalte an die Öffentlichkeit bringen und sehen sich dabei nicht als Täter. Andere wollen vielleicht aus purem Vergnügen mit begrenztem Aufwand bei irgendwem Schaden anrichten – praktisch, wenn die neue Pelletheizung ungeschützt mit dem Internet verbunden ist und im Winter von Jedermann nach Belieben umprogrammiert und ausgeschaltet werden kann. Und andere gehen organisiert und gewerbsmäßig ihren Angriffstätigkeiten nach, z. B. um Wirtschaftsspionage zu betreiben.

Behörden Spiegel: *Herr Dr. Ortner, können Gesetze gegen Cyber-Angriffe helfen?*

Dr. Ortner: Gesetzliche Regelungen selbst schützen natürlich nicht vor solchen Angriffen. Auch das Strafrecht schreckt Angreifer nicht ab, da die sich in der Regel in einem anderen Land befinden und dort eine Strafverfolgung nicht stattfindet oder nur schwer durchsetzbar ist. Sicher gibt es immer wieder Ausnahmen, siehe den Fall “Kim Dotcom”. Schützen kann man sich nur auf technische Art und Weise und vor allem durch Aufklärung.

Behörden Spiegel: *Herr Wundram, welche Möglichkeiten kann und sollte ein Unternehmen ergreifen, um sich besser zu schützen?*

Wundram: Da gibt es viele wichtige Maßnahmen und Lösungen. Klar ist, das kostet Zeit und Ressourcen, aber ohne geht es nicht mehr. Virenscanner alleine bilden dabei nicht einmal mehr die Mindestmaßnahme. Unabdingbar sind Netzwerk- und Datentrennung, sicher konfigurierte IT-Systeme und ganz besonders wichtig sind Awareness, Problembewusstsein sowie Know-how auf wirklich allen Unternehmensebenen.

Dr. Ortner: An dieser Stelle werden gesetzliche Regelungen relevant. Das Datenschutzrecht bezweckt und fordert, dass die personenbezogenen Daten im Unternehmen geschützt bleiben, das IT-Sicherheitsgesetz bezweckt, dass Betreiber besonders gefährdeter Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet werden, ihre Netze besser vor Hacker-Angriffen zu schützen.

Behörden Spiegel: *Herr Dr. Wettich, mit welchen Konsequenzen muss die Leitung eines Unternehmens rechnen, wenn es zu einem Schaden durch Hacker gekommen ist?*

Dr. Wettich: Die Unternehmensleitung, also Vorstand bzw. Geschäftsführung, muss für eine angemessene IT-Sicherheit im Unternehmen sorgen. Denn ein Mindestmaß an Schutz vor Hacker-Angriffen und Sicherung der im Unternehmen verwendeten Daten gehört zu den erforderlichen Risikovorsorgepflichten im Rahmen eines Compliance-Systems. Zusätzlich muss die Unternehmensleitung überwachen, dass die Mitarbeiter die IT-Sicherheit im Unternehmen auch tatsächlich umsetzen. Verstößt die Geschäftsleitung gegen diese Pflichten, kann ein hierdurch verursachter Schaden infolge eines Hacker-Angriffs zu einer persönlichen Haftung der Vorstände und Geschäftsführer und zu ihrer Abberufung führen. Neben der Unternehmensleitung können auch IT-Verantwortliche und Datenschutzbeauftragte im Unternehmen haften.

Behörden Spiegel: *Sind sich die Unternehmen Ihrer Erfahrung nach dieser Tatsache hinreichend bewusst?*

Dr. Wettich: Die Bedeutung des Themas IT-Sicherheit und die rechtlichen und finanziellen Folgen von Hacker-Angriffen für die Unternehmen und deren Leitung wird meiner Erfahrung nach in vielen Unternehmen immer noch unterschätzt. So verfügen eine Reihe von Unternehmen weiterhin nicht über eine konkrete IT-Notfallplanung für den Fall eines Hacker-Angriffs. In anderen Unternehmen bestehen die Prozessvoraussetzungen, jedoch mangelt es an der laufenden Überwachung, weil die persönliche Komponente unterschätzt wird. So ist neben einer funktionierenden Prozessorganisation eine gute Zusammenarbeit aller an dem Prozess beteiligten Personen, von der Unternehmensleitung bis zum Mitarbeiter, zentrale Voraussetzung einer guten IT-Sicherheit.

Behörden Spiegel: *Herr Müller, was sollte ein Unternehmen im Fall eines Hackerangriffs, der offen zutage getreten ist, tun, um seinen Ruf zu schützen?*

Müller: Hier gibt es drei Grundregeln zu beachten. Erstens gilt, das Unternehmen sollte die Öffentlichkeit umgehend informieren. Entscheidend dabei ist, dass die Information über den Angriff und die dazugehörigen Fakten zu allererst vom Unternehmen selbst bekannt gegeben werden und nicht durch Dritte, wie betroffene Kunden, eigene Mitarbeiter oder Aufsichtsbehörden.

Zweitens gilt es nicht nur die Fakten darzustellen, sondern auch den Lösungsweg aufzuzeigen: Wie kann der eventuell entstandene Schaden behoben werden? Wie kann zukünftig ein solcher Angriff verhindert werden? Daher empfehlen wir, schon im Vorfeld einen Notfallplan zu etablieren, der eben auch die kommunikativen Aufgaben im Blick hält.

Und drittens geht es darum, die Betroffenen zu informieren und festzustellen, welche Kunden und Daten waren von dem Hackerangriff betroffen. Nicht betroffene Kunden sollten ebenfalls informiert werden. Diese Informationspolitik reduziert die Unsicherheit und baut verloren gegangenes Vertrauen wieder auf. Bei kommerziellen Firmen raten wir, den betroffenen Kunden eine Kompensation anzubieten, die gleichzeitig als Bindungsinstrument funktioniert.

Seminar für IT-Entscheider

Mit einem Seminar zum Thema IT-Compliance richtet sich die Cyber Akademie speziell an Führungskräfte im IT-Bereich. Untersuchungen zeigen, dass es hier bei manchen Unternehmen durchaus Nachholbedarf gibt. Mangelnde Compliance begünstigt Cyber-Angriffe. Das Seminar gibt den Teilnehmern konkrete Handlungsempfehlungen mit auf den Weg und hilft ihnen dabei, IT-Risikofaktoren frühzeitig zu erkennen. Die hier interviewten Experten treten in dem Seminar als Referenten auf.

Mehr Informationen unter www.cyber-akademie.de

MELDUNG

Klage gegen US-Regierung

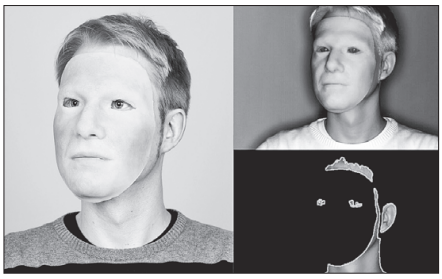
(BS) Microsoft hat die US-Regierung verklagt. Der Konzern möchte mit diesem Schritt klären, ob es verfassungswidrig ist, dass amerikanische Ermittlungsbehörden regelmäßig Geheimhaltung einfordern, wenn sie auf Daten von Microsoft-Kunden zugreifen.

Microsoft hat nach eigenen Angaben in den vergangenen 18 Monaten über 5.000 Anordnungen für digitale Durchsuchungen, etwa für Cloud-Dienste, von US-Strafverfolgern erhalten. In rund der Hälfte der Fälle wurde eine Geheimhaltung verlangt.

Biometrische Identifizierung

Forschungsprojekt zur Gesichtserkennung minimiert Fehler

(BS/th) Besonders im Hochsicherheitsbereich wie z. B. in Kernkraftwerken wird verstärkt auf die biometrische Erkennung von Personen gesetzt. Neben Fingerabdrücken geschieht dies unter anderem mit Hilfe von Gesichtserkennung.



Links ist ein Täuschungsversuch einer RGB-Kamera zu sehen. Auf der rechten Seite sind die Bilder der in dem Forschungsprojekt verwendeten NIR-Kamera zu sehen. Foto: Hochschule Bonn-Rhein-Sieg/M.Sc. Holger Steiner

Doch auch hier ist eine Manipulation möglich, da viele Kameras nicht erkennen, ob jemand eine Maske trägt oder ob es sich um ein echtes Gesicht handelt. In den Anfängen der Technologie war es möglich, mithilfe eines Fotos eine Identität vorzutäuschen.

Unter dem Titel “FeGeb, Fälschungserkennung für die Gesichtsbiometrie mit aktivem NIR-Kamerasystem” steht ein Forschungsprojekt am Institut für Sicherheitsforschung an der Hochschule Bonn Rhein-Sieg unter Leitung von *Professor Dr. Norbert Jung* kurz vor dem Abschluss. Es hat sich zum Ziel gesetzt, die Fehleranfälligkeit biometrischer Gesichtserkennung zu minimieren. Ziel ist es, echte Haut eindeutig zu erkennen. Das Bundesministerium für Wissenschaft und Forschung (BMWF) hat das Vorhaben finanziell unterstützt.

Herausforderung Hauterkennung

Personen anhand der Haut eindeutig zu identifizieren, ist aus mehreren Gründen sehr schwierig. Zum einen gibt es sehr unterschiedliche Hauttypen, darüber hinaus sind optimale Lichtverhältnisse Grundvoraussetzung für die eindeutige Identifizierung. Hautähnlich aussehende Materialien, die für Masken verwendet werden, stellen ebenfalls eine Herausforderung dar. Menschliche Haut lässt sich im Bereich des sichtbaren Lichts nicht zweifelsfrei von anderen Materialien unterscheiden.

Das Forschungsprojekt der Hochschule Bonn Rhein-Sieg setzt daher auf Nahinfrarotwellen. Der Grund für die Verwendung von Nahinfrarotwellen liegt darin, dass sich die Haut jedes Typs im nahinfraroten Bereich signifikant von anderen Materialien unterscheidet und es auf diese Weise möglich wird, Fälschungen deutlich leichter zu erkennen.

“Nahinfrarot wird oft mit Infrarot verwechselt”, so *Professor Jung,* der darauf aufmerksam machte, dass die Intensität der für das System zur Gesichtserkennung verwendeten Nahinfrarotstrahlung rund ein Zehntel dessen beträgt, was bei normaler Infrarotstrahlung üblich ist. Aus diesem Grund würden die Personen, die mithilfe der Technik identifiziert werden, die Wärme der Strahlen im Gesicht kaum spüren. Auch für die Augen ist die Methode ungefährlich. Untersuchungen hätten gezeigt, dass die für die Identifizierung verwendeten LED-Leuchten keine nennenswerte Wärmeentwicklung erzeugten. Sobald das Projekt ausgereift ist, kann es unter anderem in Form sogenannter E-Gate-Systeme an neuralgischen Punkten wie Grenzübergängen oder Fußballstadien eingesetzt werden.

Neues Forschungsvorhaben

Bei Kindern und Jugendlichen ist eine sichere Gesichtserkennung aufgrund des Wachstums auch mithilfe des Systems von *Professor Jung* und seinem Team nicht möglich. Hier müssen andere Wege zur sicheren Identifizierung gefunden werden. Das gilt für auch eine Identifizierung über den Fingerabdruck. In einem neuen Forschungsprojekt soll ein dreidimensionaler Fingerscanner entwickelt werden, mit dessen Hilfe auch Kinder und Jugendliche, z. B. im Rahmen der Flüchtlingsregistrierung eindeutig identifiziert werden können. Der Fingerscanner erfasst nicht nur die oberste Hautschicht, sondern den gesamten Finger. Auf diese Weise soll eine eindeutige Identifizierung von Kindern und Jugendlichen ermöglicht werden. Für das Projekt steht die Förderzusage des BMWF allerdings noch aus.