77500 · ISSN 1866-2420 · Einzelverkaufspreis: 12,- €

Juli/August 4/2013

SECURITY insight

Fachzeitschrift für Unternehmenssicherheit

Titelthema:

Mitarbeiter-Screening

Spitzengespräch:

Dr. Roland Weiß, R+V

Im Fokus:

Verkehr und Logistik

Drum prüfe, wer sich ewig bindet

Das Screening von Mitarbeitern ist immer ein Spagat – doch mit Rechtssicherheit, Sensibilisierung und einer soliden Vertrauensbasis lässt er sich bewältigen

Von Udo Hohlfeld

Das schwächste Glied in der Verteidigungskette ist und bleibt der Mensch. Das wissen nicht nur Militärs und Geheimdienste, sondern auch innovative Unternehmen, die ihre „Kronjuwelen" schützen müssen. Es ist somit verständlich, dass die Verantwortlichen im Unternehmen ihre Mitarbeiter „kennen" wollen – schließlich binden sie sich an sie und diese erhalten ja auch Zugang zu wichtigen und erfolgsrelevanten Interna: „Drum prüfe, wer sich ewig bindet!" Auch wenn die Bindung nicht ewig währt – in unserer globalisierten Welt mit ihren dezentralen und mobilen Medien ist die Prüfung wichtiger denn je. Für alle Unternehmen.

„Mitarbeiter-Screening", „Mitarbeiter-Überwachung", „Background-Check" – umstrittene Schlagwörter. Wie viele Daten und Informationen darf und sollte ein Unternehmen über seine Mitarbeiter erheben und speichern? Was ist mit persönlichen Informationen, die Mitarbeiter in sozialen Netzwerken wie Facebook, Xing oder LinkedIn freiwillig veröffentlichen? Für Unternehmen entstehen viele Fragen zu diesem Thema, aber auch viele Möglichkeiten, sich zu informieren oder in Fallen zu tappen. Ist es richtig, von vornherein misstrauisch zu sein sowie gegenwärtigen wie künftigen Angestellten Fehlverhalten zu unterstellen? Nein, das wäre kein guter Start für eine langfristige und vertrauensvolle Zusammenarbeit. Und der Generalverdacht ist in Deutschland ohnehin verboten – aus guten Gründen!

Negativbeispiel

Der Umgang mit personenbezogenen Daten ist durch das Bundesdatenschutzgesetz (BDSG) geregelt. Nach § 4 Abs. 1 ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur

dann zulässig, wenn das BDSG oder andere Rechtsvorschriften dies erlauben oder anordnen oder betroffene Personen darin eingewilligt haben.

Ein bekanntes Negativbeispiel ist die Rasterfahndung der Deutschen Bahn AG unter ihren Angestellten: Von 2002 bis 2005 hat der Konzern ohne konkreten Anlass heimlich Daten vieler Mitarbeiter sowie ihrer Angehörigen mit Daten von Lieferanten abgeglichen. Angeblich zum Zweck der Korruptionsbekämpfung. Es wurde weiterhin eine professionelle Detektei beauftragt, Kontodaten von Angestellten zu identifizieren. Die Bahn hat diese Daten über Jahre hinweg gespeichert. Mitunter wurden sogar Kontoinformationen über Familienangehörige erhoben und in den Auswertungen mitverwendet. 2009 dann akzeptierte die Deutsche Bahn ein Rekordbußgeld von rund 1,12 Millionen Euro, womit all ihre aufgedeckten Datenschutzverstöße geahndet wurden. Was hat es dem Unternehmen letztlich gebracht – außer Imageschaden und dem Vertrauensverlust der Mitarbeiter?

Persönlich kenne ich den „Background-Check" aus der akademischen Welt. Für die Zulassung zu meinem Studium an der American Military University musste ich in einen Background-Check einwilligen. Polizeiliches Führungszeugnis, zwei Referenzen (zwecks Charakterprüfung meiner Person) – das waren die Bestandteile; wahrscheinlich wurde ich noch mit einer Liste von Terrorismusverdächtigen oder gesuchten Kriminellen abgeglichen. Da ich kurz vor Beendigung meines Studiums (Master of Strategic Intelligence) stand, ist damals wohl alles glatt gelaufen. In Zeiten von „Tempora" und „Prism" scheint mir dieses Vorgehen eher als unnötige Bürokratie und ein Relikt der alten Zeit.

Stichwort „Terrorismus": Es ist in der internationalen Unternehmenswelt bereits gängige Praxis, Mitarbeiternamen mit Namenslisten abzugleichen, die terrorismusverdächtige Personen und Organisationen erfassen. Auch hier gibt es Regeln, und es gilt wieder § 4 Abs. 1 BDSG. Zumal es klar sein sollte, dass ein Abgleich mit diesen Listen sicherlich nicht dem Arbeitsverhältnis dienlich ist. Bei der Abwägung von Unternehmens- gegen Mitarbeiterinteressen stehen immer die schutzwürdigen Interessen des betroffenen Mitarbeiters im Vordergrund. Solche Listen und ihr Ursprung basieren nicht immer auf gesetzeskonformen Kriterien, vor allem, wenn sie im Ausland erstellt wurden.

Von Mäusen und anderen Schwachstellen

Horst K., ein fiktiver Angestellter der fiktiven Firma „Hochsicherheitstechnologie GmbH", ist ein zuverlässiger und wertvoller Mitarbeiter. Er arbeitet in der Entwicklungsabteilung, schon seit zehn Jahren. K. hat einen USB-Stick voll mit Informationen über die neue Produktentwicklung an einen asiatischen Konkurrenten verkauft. Warum? Er hat ein krankes Kind, und die Arztkosten verschlingen Unsummen. K. wollte nur, dass sein Kind endlich wieder gesund wird.

MICE ist ein Akronym und steht für die englischsprachigen Begriffe *M*oney (Geld), *I*deology (politische Überzeugung), *C*ompromise (Kompromittierung) und *E*go – vier Beweggründe, warum Mitarbeiter ihren Arbeitgeber schädigen. Manche benötigen viel Geld für ihren Lebensstil oder, wie Horst K., für finanzielle Extremsituationen. Andere wiederum sind Überzeugungstäter, die einer bestimmten Ideologie nahestehen und diese bestmöglich unterstützen möchten. Es gibt auch Mitarbeiter, die bewusst in dokumentierte, kompromittierende Situationen gebracht und damit erpresst werden (siehe Titelthema „Sex & Security" in SI 2/13). Andere Mitarbeiter leiden unter einem verletzten Ego – sie wurden bei der Beförderung übergangen, vor Kollegen bloßgestellt oder ungerecht behandelt. Rache ist ihre Medizin, um das verletzte Ego wieder aufzubauen. Wer erinnert sich nicht an den Ferrari-Mitarbeiter Nigel Stepney, der nach einer Reorganisation des Formel-1-Teams zum Alteisen aussortiert wurde und sich mit dem Verrat von Konstruktionsdaten ans McLaren-Mercedes-Team dafür bedankte?

Doch mal direkt gefragt: Welcher der vier MICE-Typen kann überhaupt frühzeitig per Background-Check identifiziert werden? Was ist eigentlich Sinn und Zweck von Mitarbeiter-Screening oder generell der Überwachung von Mitarbeitern am Arbeitsplatz? Vordergründig wird wohl jeder bestätigen, dass es um Sicherheit für das Unternehmen geht. Bei genauerer Betrachtung jedoch ergibt sich ein anderes Bild: Misstrauen und Unsicherheit auf Seiten des Unternehmens, das seine Wettbewerbsfähigkeit gefährdet sieht. In der Tat gibt es vermehrt Berichte über Mitarbeiter, die ihren Arbeitgeber geschädigt haben und noch mehr Vorfälle, die sicher nie öffentlich werden.

Der Terminus „Vorfälle" umfasst dabei alles, was einem Unternehmen schadet: vom einfachen Diebstahl über Unterschlagung bis hin zu Geheimnisverrat und Spionage. Der „2013 Data Breach Investigations Report" *(www.verizonenterprise.com/DBIR/2013)* zeigt, dass 14 Prozent der untersuchten Vorfälle von Mitarbeitern begangen wurden – vor allem aus finanziellen Beweggründen.

SI-Autor Udo Hohlfeld ist Competitive Intelligence und Counterintelligence Specialist und Geschäftsführer der Info + Daten GmbH & Co. KG (www.infoplusdaten.net). Das Unternehmen hat sich darauf spezialisiert, für seine Kunden strategische Erkenntnisse über Wettbewerber, Produkte und Märkte zu beschaffen und gleichzeitig sich selbst zu schützen.

Schwachstelle	Signifikanz
Mitarbeiter	
persönliche, finanzielle Situation	hoch
verletztes Ego	hoch
Erpressung	mittel
Social Engineering	hoch
fehlende Sensibilisierung für Unternehmenssicherheit	hoch
Unternehmen	
fehlende Sicherheitsrichtlinien	mittel
falsch konfigurierte Systeme	hoch
fehlende/mangelhafte Mitarbeiterschulung	hoch
unzureichende technische Schutzmaßnahmen	hoch

Mögliche Schwachstellen eines Unternehmens

Geschäftspartner waren für lediglich ein Prozent der Vorfälle verantwortlich. Die restlichen Vorfälle gehen aufs Konto externer Akteure oder einem Mix interner und externer Akteure. Zur Rettung des Rufs der Mitarbeiter muss darauf hingewiesen werden, dass die Taten nicht immer vorsätzlich begangen wurden. Falsch konfigurierte Systeme, Nachlässigkeit bei der Arbeit oder laxe Unternehmensregeln für den Umgang mit sensiblen Daten verursachen ebenso Schaden und sind in dem 14-Prozent-Wert enthalten.

Drei Beziehungsphasen

Knackpunkte sind die unterschiedlichen Interessenslagen. Auf der einen Seite muss sich ein Unternehmen schützen. Auf der anderen Seite steht der Angestellte, der seine Privatsphäre und Integrität schützen möchte. Die Beziehung zwischen Unternehmen und ihren Mitarbeitern kann in drei Phasen unterteilt werden. Phase 1 umfasst Bewerbung und Anstellung, Phase 2 entspricht dem eigentlichen Beschäftigungsverhältnis, und Phase 3 schließlich beginnt mit der Beendigung des Beschäftigungsverhältnisses.

Phase 1

Unternehmen sollten grundsätzlich die Angaben von Bewerbern überprüfen. In Lebensläufen wird oft geschönt oder glatt gelogen. Diese Überprüfung ist aber nur möglich, wenn der Bewerber dazu sein schriftliches Einverständnis gibt. Hier findet direkt die Trennung der Spreu vom Weizen statt. Es ist klar, dass nicht nur der seine Bewerbung zurückzieht, dem die Überprüfung schaden würde, sondern auch der, dem diese Praxis seines potenziellen Arbeitgebers nicht zusagt. Auch darf ein (potenzieller) Arbeitgeber im Internet über einen Bewerber oder Mitarbeiter recherchieren. Einschränkung ist, dass diese Recherche relevant sein muss für die Entscheidung über Einstellung oder Versetzung auf eine andere (sicherheitsrelevante) Stelle. Selbstverständlich darf überprüft werden, ob Angaben aus dem Lebenslauf stimmen. Eindeutig verboten ist, in sozialen Netzwerken unter falschen Angaben Kontakt zum Bewerber oder Mitarbeiter herzustellen, um an weitere persönliche Daten zu gelangen.

Phase 2

In dieser Phase werden mitarbeiterbezogene Daten gespeichert: für die Gehaltsabrechnung, den Austausch mit der Krankenkasse oder dem Finanzamt oder die interne Karriereplanung. Ein Arbeitgeber darf aber auf keinen Fall Daten über die politische Einstellung, die Zugehörigkeit zu Organisationen, sexuelle Vorlieben, Krankheitsdiagnosen oder ethnische Herkunft speichern oder gar verwenden. Arbeitsausfallzeiten dürfen aus der Gehaltsabrechnung berechnet werden, aber nur im Einzelfall und nicht, um mehrere Mitarbeiter miteinander zu vergleichen. Berufliche E-Mails dürfen zur Überprüfung der Arbeit verwendet werden. Dafür dürfen Programme eingesetzt werden, die den Inhalt auf Schlagworte wie „Porno“, „Sex“ usw. überprüfen, um Missbrauch zu erkennen. Telefonate dürfen grundsätzlich nicht mitgehört oder aufgezeichnet werden.

Wichtig ist hier, was zwischen Unternehmen und Mitarbeiter im Arbeitsvertrag vereinbart wird, gerade in Bezug auf die Internetnutzung, private E-Mails und Telefonate. Ähnlich strikt ist der Umgang mit der Videoüberwachung. Lidl und Schlecker kennen sich da bestens aus. Die Nutzung von Kameras in Sozialräumen, Umkleideräumen oder Toiletten ist verboten. Die offene Videoüberwachung wiederum ist erlaubt – wenn die Mitarbeiter darüber vorab informiert wurden. Die offene Videoüberwachung von Verkaufs- und Ausstellungsflächen ist ebenso erlaubt und muss von Mitarbeitern akzeptiert werden. Erst bei einem konkreten Anlass – etwa signifikante Pflichtverletzungen oder sogar Straftaten – ist der automatische Abgleich von Mitarbeiterdaten in anonymisierter Form erlaubt. Dessen Resultate dürfen bei Verdacht dann auch einzelnen Mitarbeitern zugeordnet werden.

Phase 3

Wenn das Beschäftigungsverhältnis beendet wird, müssen viele Mitarbeiterdaten vernichtet werden, es sei denn, sie werden für Unternehmensprüfungen benötigt und ihre Speicherung ist gesetzlich vorgeschrieben. Oft ist es auch so, dass Mitarbeiter Daten mitnehmen, sei es um sich bei ihrem neuen Arbeitgeber Vorteile zu verschaffen, sei es um sich einfach für etwas zu rächen. Unternehmen haben es in diesen Fällen in der

Wenn Mitarbeiter private Sorgen haben, sollten Arbeitgeber helfen, so es in ihrer Macht steht. Letztlich ist dies eine Investition in die Unternehmenssicherheit.

Bei aller Vorsicht gegenüber Mitarbeitern sollte man nicht vergessen: Es sind vor allem Externe, die Unternehmen schädigen.

Hand, dem Fehlverhalten durch technische Restriktionen und vorbeugendes Handeln frühzeitig einen Riegel vorzuschieben.

Empfehlungen

Es braucht definitiv Rechtssicherheit für Unternehmen und Mitarbeiter für den Umgang mit den Beschäftigtendaten sowie der fallbezogenen Überwachung. Mitarbeitern muss klar gemacht werden, dass sie Pflichten gegenüber ihrem Arbeitgeber haben. Diese Gesetze und Regeln greifen natürlich nur, wenn das Kind schon in den Brunnen gefallen ist. Unabhängig davon braucht es eine Vertrauensbasis zwischen Unternehmen und Beschäftigten, gegenseitige Fürsorge und Respekt sowie „maßvolle Überwachung" – nicht aus Angst und Misstrauen, sondern zum Schutz aller Beteiligten. Im Sinne eines guten Betriebsklimas ist sicherlich nicht jede Überwachungsmaßnahme und jedes Screening sinnvoll. Für die Vorbeugung von Schaden ist es wichtig, die Mitarbeiter zu sensibilisieren und aktiv einzubinden. Unternehmen und Mitarbeiter ziehen letztlich an einem Strang für den gemeinsamen Erfolg.

Zu den Grundlagen dafür gehören neben einer fairen, vertrauensvollen Unternehmenskultur auch die Aufklärung der Mitarbeiter über Kontrollen und punktuelle Überwachungsmaßnahmen, die Schulung der Mitarbeiter im Umgang mit sensiblen Daten, Umsetzung sicherer Prozesse und technischer Maßnahmen für Informations- und Datensicherheit und *last but not least* funktionierende, sichere Systeme. Wichtig ist auch, dass es für Mitarbeiter, die in Problemen stecken – welcher Art auch immer, siehe MICE –, betriebliche Ansprechstellen gibt, die helfen dürfen und können.

Mitarbeiter sollten offen sein für das Sicherheitsbedürfnis ihres Arbeitgebers und im Zweifel nachfragen, damit keine Unsicherheit oder Missverständnisse entstehen. Wenn sie mit Problemen kämpfen, sollten sie vertrauensvoll Hilfsangebote des Unternehmens nutzen. Schulungsangebote des Arbeitgebers sind Pflichtprogramm, ebenso das Melden von Verdachtsmomenten.

Das hört sich idealistischer an, als es ist. Die Umsetzung bringt Hürden mit sich, und schwarze Schafe wird es immer geben. Doch sie sind die „große Minderheit" und dürfen nicht der Grund dafür sein, dass Unternehmen ihre Belegschaft unter Generalverdacht stellen und mit Methoden von Überwachungsstaaten ausspionieren. Motivierte Mitarbeiter sind die Erfolgsgaranten eines Unternehmens, und die sollten gepflegt und gefördert werden – Vertrauen ist hier besser als pauschale Kontrolle.