BEILAGE ZUM DSD 1 | 2016

BDSW

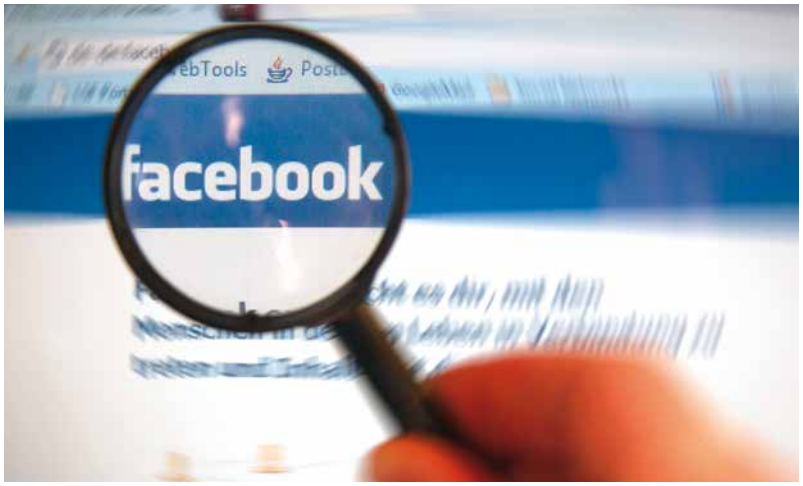
INFO WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Licht und Schatten

SOZIALE NETZWERKE HABEN VIELE GUTE SEITEN. Kaum jemand verzichtet deshalb auf die Möglichkeit, sich mit anderen Menschen zu vernetzen. Aber wie immer im Leben: Wo viel Licht ist, ist auch viel Schatten. Segen und Fluch liegen oftmals dicht beieinander. Die sozialen Netzwerke haben definitiv auch ihre dunklen Seiten, die nicht verschwiegen werden sollten.

Wohlgemerkt: Soziale Netzwerke sind – wie schon eingangs erwähnt – durchaus nichts Schlechtes, weder für die Mitarbeiter noch für die Unternehmen. Aber wie in der Heilkunde gelten die Devisen: „Die Dosis macht das Gift" und „Allzu viel ist ungesund". Prüfen Sie deshalb, welche Inhalte wirklich in ein Profil gehören, auf das Milliarden von Nutzern zugreifen können. Allein Facebook hat nach 2015 vorgelegten Daten weltweit 1,5 Milliarden Nutzer. Das ist fast ein Fünftel der Weltbevölkerung und das nur in einer einzigen Online-Community. Hand aufs Herz: Muss diese gigantische unüberschaubare Anzahl von Menschen alles über eine Einzelperson in Deutschland wissen?



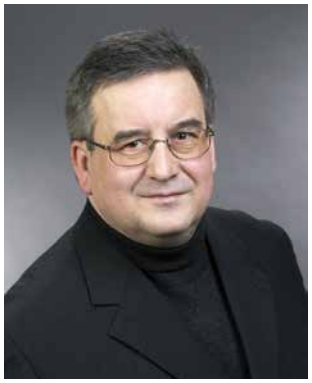
1,5 Milliarden Nutzer gibt es weltweit allein bei Facebook. Eine ideale Basis, um aus jedem Winkel unserer Erde Informationen über Personen zu sammeln.
Foto: Alexander Klaus / pixelio.de

Es ist wie beim Messer. Niemand verurteilt es, wenn damit Brot geschnitten wird. Aber im Hinterkopf muss immer auch die Option beachtet werden, dass es als Waffe dienen kann. Ein Vergleich, der auch auf Social Media zutrifft. In den falschen Händen können auch sie als Waffe eingesetzt werden. Nämlich, um aus kriminellen Motiven sensible Informationen über Unternehmen und deren Mitarbeiter zu erlangen.

Zweifelsohne: Es steht in vielen Profilen weitaus mehr als notwendig ist. In den sozialen Medien wird überdeutlich, dass datenschutzmäßig mit zweierlei Maß gemessen wird. Während im realen Leben im übertragenen Sinne um jeden Buchstaben gerungen wird, werden in der virtuellen Welt von Facebook, Twitter, Xing, LinkedIn & Co. komplette Autobiografien preisgegeben. In sozialen Netzwerken vertreten zu sein, gilt nicht als Kür, sondern eher als Pflicht. Schon 2009 schrieb ein Journalist der ZEIT, man gelte langsam als Sonderling, wenn man nicht mitmache, „vergleichbar jenen Menschen, die einst zögerten, sich ein Handy anzuschaffen". In der Tat werden vielfach Accounts nur deshalb eingerichtet, weil es die Mehrheit im Unternehmen so hält, und sich kaum jemand gerne ausschließt.

Social Media – ja. Aber nicht ohne Vorsichtsmaßnahmen. Das ist die Quintessenz unseres heutigen Beitrages zu dieser Thematik.

Ihr
Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz



Risiken der Social Media

Weshalb ein paar Mausklicks reichen, um komplette Personenprofile zu erstellen

Von Klaus Henning Glitza

SPIONE ALLER SCHATTIERUNGEN LIEBEN SIE, die sozialen Netzwerke. Schließlich stellen sie eine wesentliche „Arbeitserleichterung" dar. In früheren Zeiten waren noch aufwändige Recherchen erforderlich, um an bestimmte Informationen über Personen zu kommen. Dagegen reichen heute oft ein paar Mausklicks aus, um komplette Personenprofile zu erstellen. „Selbst Leute, die energisch den Schutz ihrer Daten einfordern, geben oft bedenkenlos und völlig ohne Not personenbezogene Daten im weltweiten Netz preis", so ein Insider.

Angenommen, ein Wirtschaftsspion oder Konkurrenzausspäher möchte Informationen über ein Unternehmen gewinnen. Neben allgemeinen Daten, die im Internet recherchierbar sind, spielen oft auch die Namen der Mitarbeiter eine Rolle. Deren Kenntnis eröffnet die Chance, die Beschäftigten zu kontaktieren und ihnen, vielfach auf dem Wege der Abschöpfung, nichtöffentliche Informationen zu entlocken. Das ist letztlich auch für Mitarbeiter von hohem Risiko. Erst einmal im Visier fremder Dienste und Konkurrenzspione, werden sie schnell in Zusammenhänge verstrickt, die sie nicht mehr kontrollieren können.

Soziale Netzwerke eignen sich für diese finsteren Zwecke ideal. Der Spion beziehungsweise Späher kann sich unter einem erfundenen Namen oder dem Namen einer fremden Person problemlos einen Fake-Account einrichten. Kaum ein „Social Medium" überprüft die Identität der Nutzer. Diverse Untersuchungen haben ergeben, dass gefälschte Profile keinesfalls eine Seltenheit sind.

Um nicht von Anfang an aufzufallen, verschafft sich der informationshungrige Angreifer im Schnelldurchgang ein paar Kontakte, bei Facebook „Freunde" genannt. Die meisten Kontaktwünsche werden üblicherweise mit einem gewissen Automatismus bestätigt, ohne dass die Identität des Anfragenden überprüft wird. Smarte Späher richten mehrere Accounts unter Falschnamen ein und vernetzen diese dann miteinander. So können hochrangige Kontakte wie Präsident, Geschäftsführer oder Vorstandsvorsitzender vorgetäuscht werden. Die Angreifer wissen genau, dass sich kaum jemand die Mühe macht, die Echtheit zu überprüfen.

Nach diesen vorbereitenden Schritten werden in den Online-Communities gezielt Mitarbeiter des interessierenden Unternehmens gesucht. Oft haben Unternehmen selbst Profile in soziale Netzwerke gestellt. Die Firmenangehörigen lassen sich dann im Regelfall über die öffentlich sichtbaren „Gefällt mir"-Angaben, die so genannten Likes, feststellen. Sind erst einmal Beschäftigte identifiziert, führt deren Kontaktliste meist zu weiteren Mitarbeiterinnen und Mitarbeitern. In einigen sozialen Netzwerken ist aber so viel Mühe gar nicht nötig. Es genügt, den Firmennamen einzugeben und schon werden die Namen aufgelistet.

Jetzt muss sich der Spion nur noch die einzelnen Accounts genauer ansehen. Erfahrungsgemäß wird er sein Augenmerk auf Positionen richten, die für seine „Beschaffungsziele" günstig erscheinen. Das müssen nicht unbedingt Führungskräfte sein. Mitarbeiter fremder Nachrichtendienste haben, so die Auswertung früherer Fälle, bevorzugt Sekretärinnen ins Visier genommen und tun dies wohl auch heute noch. Auch der Hausbote, die Empfangsdame, die Telefonistin oder die Kantinenkraft können sprudelnde Quellen sein. Es geht nicht um die Stellung in der Hierarchie, sondern um bestmögliche Zugangsmöglichkeiten zu sensiblen Informationen.

Ein zweiter Schritt des Spions könnte darin bestehen, verräterische Kennzeichen für berufliche Veränderungswünsche zu identifizieren. Diese Indikatoren sind in sozialen Netzwerken nur schwach verschleiert. Wenn jemand eine „neue Herausforderung" oder eine Führungsposition (obwohl aktuell auf der Arbeitsebene tätig) sucht, ist dies ein untrügliches Zeichen dafür, dass ein neuer Arbeitsplatz gesucht wird. Manche Social Media-Nutzer aber gehen vorsichtiger vor. Sie preisen einfach nur ihre Fähigkeiten und Expertise an, um auf diesem Wege Headhunter und Mitarbeiter suchende Arbeitgeber auf sich aufmerksam zu machen. Aufmerksam werden dadurch aber auch Andere, die das Selbstlob wohl zu werten wissen.

Des Weiteren wird, so zeigen bisherige Fälle, nach sehr persönlichen Informationen geforscht. Welche Hobbys oder sonstige Vorlieben eine Person hat, steht oft schon in sozialen Medien, in denen überwiegend Manager und andere Angestellte vertreten sind. Jeder weiß es aus Bewerbungsgesprächen, dass fast immer nach den Hobbys gefragt wird, um einen Kandidaten besser einschätzen zu können. Unter anderem aus diesem Grund

Verräterische „Gefällt-mir"-Angaben: Auf Unternehmensseiten in sozialen Netzwerken führen die so genannten Likes zwangsläufig zu den Mitarbeitern. In privaten Profilen outen sie, welche Vorlieben die betreffende Person hat. Foto: Tim Reckmann / pixelio.de

Wirtschaftsspionage 2.0 im digitalen Zeitalter: Von einem Personenprofil sind Angreifer nur ein paar Tastenanschläge entfernt. Foto: Petra Bork / pixelio.de

beantworten viele Nutzer diese Standardfrage der Personaler in vorauseilender Art bereits, bevor sie gestellt wird, aber auch, weil es andere auch so halten.

Die genannten Hobbys sind maßgebliche Mosaiksteinchen für ein Personenprofil. Kaum ein Thema eignet sich besser als Türöffner, als ein angeblich gemeinsames Hobby. Jemand, der wie zufällig in ein Gespräch einfließen lässt, dass er derselben Freizeitbeschäftigung nachgeht, wirkt gleich um mehrere Faktoren sympathischer. Kurzum: Für Spione aller Schattierungen sind solche Informationen Gold wert.

In einigen Social Media kann aber noch viel mehr in Erfahrung gebracht werden als die jeweiligen Steckenpferde. Zum Beispiel das Geburtsdatum, das häufig in Internet-Netzwerken für Studenten oder in Online-Communitys zur Suche nach früheren Freunden zu finden ist. Ganz abgesehen von der Preisgabe der besuchten Schule und/oder Uni. Diese Informationsfülle wird aber noch von einigen Social Media getoppt, wo die Nutzer sogar aus freien Stücken angeben, mit wem sie verheiratet, liiert oder befreundet sind. Zumindest Tag und Monat des Geburtstages lassen sich häufig erkennen, weil Personen aus der Freundesliste just an diesem Tag, für jeden sichtbar, Gratulationsadressen verschicken. Nicht selten werden auch Urlaubsbilder in das virtuelle Netzwerk eingestellt, die öffentlich signalisieren, wohin die Reise ging. Ob Mallorca oder Bali, ob Pauschalreise oder Individualurlaub, das allein sagt schon viel über die Menschen aus. Darüber hinaus werden heutzutage gerne Fotos von Partys oder anderen Events direkt per Smartphone auf das Profil geschickt. Ein Blick in die Freundesliste spricht gleichfalls Bände. Korrespondiert die interessierende Person öffentlich mit anderen Nutzern, kann ein cleverer Spion Charaktereigenschaften, Gesinnungen, Schreibstil und die Intensität der Freundschaft mit den Kontakten erkunden.

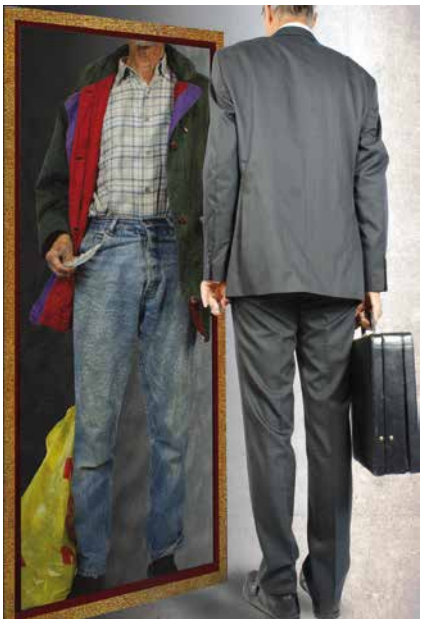
Fatal, wenn Informationen dieser Art in falsche Hände geraten. Allein aus diesen Mosaiksteinchen lassen sich bereits Dossiers über einzelne Personen erstellen. Vorlieben, aber auch Schwachpunkte lassen sich mühelos aus den selbst preisgegebenen persönlichen Interna ableiten. Selbst harmlos wirkende Informationen können viel über die jeweilige Persönlichkeit aussagen. Beispiel: Ist ein Mitarbeiter im Unternehmen auf der ganz normalen Arbeitsebene tätig, im Privatleben aber Vereinsvorsitzender, kann zumindest vermutet werden, dass seine Fähigkeiten im Betrieb unterschätzt werden. Führende Funktionen, die im deutlichen Gegensatz zu beruflichen Positionen stehen, sind oft ein Indiz dafür, dass nach einer Kompensation für Unterforderung und mangelnde Wertschätzung im Beruf gesucht wird. Ein cleverer Spion wird solche Hinweise geschickt für seine Zwecke nutzen.

Was also tun? In erster Linie gilt es, die preisgegebenen Informationen auf das Notwendigste zu beschränken. Ist es wirklich erforderlich, den gesamten Lebenslauf ins Netz zu stellen, oder genügt es nicht etwa, die aktuelle Position zu beschreiben? Ist es opportun, jeder Gruppe beizutreten, denn über Gruppen erfolgen erfahrungsgemäß besonders viele Fake-Anfragen. Machen Sie von den Privacy-Einstellungen Gebrauch und ermöglichen Sie ausschließlich Ihren geprüften oder persönlich bekannten Kontakten auf Ihre Freundesliste zuzugreifen. Nutzen Sie auch die Funktion, die so genannten Likes, die ausgesprochen aufschlussreich sein können, zu verbergen. Vermeiden Sie öffentlich sichtbare Kommentare und bevorzugen Sie Private Nachrichten (PN), die nicht von aller Welt gelesen werden können. Bitten Sie auch Ihre Kontakte, mit Ihnen ausschließlich über die PN-Schiene zu kommunizieren. Schließlich sind deren Nachrichten privat und sollten deshalb auch auf dieser Ebene gehalten werden.

Welche Warnzeichen gibt es, das eine andere Person aus dolosen Motiven mit Ihnen in Verbindung treten will? Das sicherste Indiz ist die unerwartete und unzureichend begründete Kontaktaufnahme eines unbekannten Menschen. Dümmste Begründung: „Ich bin zufällig auf Ihr Profil gekommen." Bei der Auswahl Ihrer Kontakte sollten Sie unbedingt, wie das Wort schon sagt, wählerisch sein. Sie haben es schließlich nicht nötig, Anderen mit einer Vielzahl von Kontakten zu imponieren. Es gilt die alte Regel: Kontakte sollte man nicht zählen, sondern wägen.

Checken Sie also, wer da mit Ihnen in Kontakt treten will. Gibt es diese Person wirklich? Wird ein realer Name, Stichwort Identitätsdiebstahl, verwendet, helfen kurze Internetrecherchen weiter. Hat die Person, deren Identität missbraucht wird, noch andere Profile, die eventuell von den Angaben des Kontaktsuchenden abweichen?

Möglicherweise hilft Ihnen auch das Foto des Anfragenden weiter. Oft werden die Fake-Accounts mit Bildnissen von bezaubernd schönen Menschen garniert, um die ästhetischen Sinne der Zielperson anzusprechen. Diese Fotos stammen eventuell irgendwo aus dem Internet,



Wer ist das digitale Gegenüber? Manager oder Fake? In sozialen Netzwerken kann man sich ohne Nachprüfung überhaupt nicht sicher sein. Foto: Bernd Kasper / pixelio.de

Ein Stellengesuch in einem Printmedium? Das ist meist nicht gerade billig und könnte auch dem werten Chef auffallen. Viele Nutzer von sozialen Netzwerken weisen deshalb in ihren Profilen, schwach verschleiert, auf ihre Veränderungsbereitschaft hin. Das wissen nicht nur Headhunter, sondern auch Spione für ihre Zwecke zu nutzen. Foto: Beate Klinger / pixelio.de

da die Spione kaum ihr eigenes Konterfei verwenden werden. Hier können Sie eine nützliche Funktion der Suchmaschine Google nutzen. Speichern Sie das relevante Foto auf Ihren PC und laden Sie es anschließend in Google-Bildersuche. Das funktioniert auf ganz unkomplizierte Weise: Wenn Sie Google öffnen, sehen Sie oberhalb des Google-Emblems den Button Bilder. Diesen anklicken. Es erscheint am rechten Rand des Suchfeldes ein Kamera-Symbol. Wird dieses angeklickt, öffnen sich die Auswahloptionen „Bild-URL einfügen" und „Bild hochladen". Wählen Sie Letzteres aus und laden Sie einfach das relevante Foto hoch. Es werden dann identische oder ähnliche Bilder angezeigt. Diese Funktion ist keinesfalls perfekt, stellt aber auch in anderen Fällen (Beispiel: Sie wollen die Herkunft eines Bildes überprüfen, um keine Rechte zu verletzen) eine gute Hilfe dar.

Seien Sie vor allem misstrauisch, wenn jemand allzu schnell auf den Punkt kommt und etwas über Ihr Unternehmen wissen will. Prüfen Sie dann unbedingt, ob der Anfragende wirklich die behauptete Expertise besitzt, indem Sie ihn zu einem Fachthema um Rat bitten. Und ganz wichtig: Behalten Sie Unternehmensinterna immer für sich.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

BKA-Ergebnisbericht Hacktivisten

Im Rahmen des Forschungsprojektes Hacktivisten wurden letztes Jahr ca. 4.500 Unternehmen sowie öffentliche Einrichtungen zum Thema Hacktivismus und Cybersicherheit befragt. Mit einer Rücklaufquote von 21 Prozent nahmen über 970 Unternehmen und öffentliche Einrichtungen an dieser Befragung teil. Die Verteilung der Größen und Branchenzugehörigkeit der Unternehmen entspricht weitgehend der Gesamtverteilung aller Unternehmen in Deutschland. Insofern sind die Ergebnisse hinreichend belastbar. **www.bka.de**

NIFIS-Studie: 2016 mehr Investitionen in IT-Sicherheit

Laut einer Studie von NIFIS werden die Ausgaben für IT-Sicherung und Datenschutz steigen. Mehr als die Hälfte der deutschen Firmen (53 Prozent) rechnet damit, dass die Investitionen in 2016 weiter zunehmen werden. 44 Prozent gehen von einer Steigerung um mindestens ein Drittel aus. Dies ist als Reaktion auf zunehmende Bedrohungen der deutschen Wirtschaft durch Cyberkriminalität und Wirtschaftsspionage zu werten. **www.nifis.de**

BSI: Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes

Am 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft getreten. In diesem Zusammenhang gibt es eine Reihe von Fragen wie z. B.: Für wen gilt das Gesetz? Wer ist Betreiber kritischer Infrastrukturen? Welche Betreiber kritischer Infrastrukturen unterliegen ab sofort den Regelungen des Gesetzes? Müssen IT-Standards ab sofort erfüllt werden? Auf diese und weitere Fragen gibt das BSI detaillierte Antworten. **www.bsi.bund.de**

Sicherheit für IT-Unternehmen das Thema des Jahres

Dies ergab die jährliche Trendumfrage des Digitalverbands Bitkom. Wie bereits vor zwei Jahren liegt das Thema IT-Sicherheit mit 59 Prozent der Nennungen an der Spitze. Dahinter folgen die Themen Cloud Computing, Industrie 4.0 und Internet der Dinge. **www.bitkom.org**

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Henning Glitza

Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580

Mail: mail@bdsw.de
Web: www.bdsw.de