BEILAGE ZUM DSD 4 | 2019

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Wenn sich Hintertüren öffnen

→ Die raffinierteste Angriffstechnik wäre in den meisten Fällen wirkungslos, wenn es nicht Menschen gäbe, die eine Hintertür öffnen. Nahezu jede technisch basierte Attacke auf ein Unternehmen glückt nur deshalb, weil ein Mitarbeiter etwas getan hat, was er besser unterlassen hätte. So etwas passiert meist aus Unwissenheit, häufig aber auch aus „Wurschtigkeit" oder schlicht Faulheit.

Typische Beispiele für folgenreiches menschliches Fehlverhalten sind das Öffnen von Anhängen in E-Mails von unbekannten Absendern oder sorgloses Ausplaudern von Interna. Gegen diese und andere Gefahren gibt es nur ein wirksames Mittel: die Sensibilisierung der Mitarbeiter.

Damit dieser Schritt auch gelingt, bedarf es einiger Grundbedingungen. Langweilige Vorträge sind nicht geeignet, die Mitarbeiter zu erreichen. Das gilt auch für Monologe – die Mitarbeiter sollten im Sinne der Interaktion einbezogen werden. Auch die Platzierung des Themas als Punkt X in einer Betriebsversammlung ist nicht optimal. Ebenso ist Sicherheit, die von oben herab angeordnet und deshalb bestenfalls mechnisch abgearbeitet wird, nicht der richtige Weg. Sensibilisierung ist kein Selbstläufer. Man kann viel falsch machen und damit wichtige Chancen vertun.

Ein oft zu beobachtender Fehler ist auch, das Thema nur einmal aufzugreifen und dann nie wieder. Einmal ist keinmal, heißt es. Und das trifft in vollem Maße auch auf die Sensibilisierung zu – Bedrohungen gibt es ständig und deshalb dürfen Gegenmaßnahmen nicht einmalig sein.

Doch Sensibilisierung ist kein einfaches Unterfangen. Nach dem Automatenprinzip – oben wird die Info eingeworfen, unten kommt ausgeprägtes Sicherheitsbewusstsein heraus – geht hier nichts. Deshalb möchten wir Ihnen in der heutigen Ausgabe ein paar Tipps geben. Bleiben Sie auf der sicheren Seite!

Ihr Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz ←

Jede Neuerung ruft Antihaltungen hervor. Ein Industriemagnat sagte einmal, wäre es nach den Bedenken der Menschen gegangen, hätten wir heute statt Autos schnellere Pferde.
Foto: Gabi Hamann / pixelio.de

Unternehmenssicherheit: Es kommt auf das Bewusstsein der Mitarbeiter an

Von Klaus Henning Glitza

→ Jede Art von Unternehmenssicherheit ist nur so gut wie das Sicherheitsbewusstsein der Mitarbeiter. Auch die ausgefeiltesten Sicherheitsmechanismen bleiben unwirksam, solange es Betriebsangehörige gibt, die bewusst oder unbewusst alle Sicherheitsbemühungen unterlaufen.

Der Mensch ist das Maß aller Dinge – auch bei Angriffen auf Unternehmen. Beispielsweise ist das berüchtigte Hacken ohne meist unwissentliche Mithelfer in den Unternehmen bei gut gesicherten Systemen gar nicht möglich. Um in das IT-System einzubrechen, muss erst jemand einen Mailanhang trotz unbekannter Absenderadresse geöffnet oder (Stichwort Social Engineering) sein Passwort preisgegeben haben. Oder jemand hat bei Konferenzen, Tagungen, Kongressen oder Schulungen in „geselliger Runde" Interna preisgegeben. Die Technik allein ist nichts, wenn nicht jemand eine Hintertür öffnet. Selbst Fort Knox wäre eine schwache Bastion, wenn es dort Mitarbeiter gäbe, die unachtsam zu Werke gingen.

Die konsequente Befolgung einiger weniger Sicherheitsrichtlinien kann dagegen wahre Wunder vollbringen. Deshalb ist es mehr als wichtig, in Unternehmen – egal welcher Art und Größe – Mitarbeiter zu Verbündeten in puncto Sicherheit zu machen. Und sie quasi als menschliche Firewall, die nicht nur gegen IT-Sicherheitsrisiken wirkt, in Stellung zu bringen. Dies zu realisieren, liegt allein in der Verantwortung der Unternehmen. Während beim Arbeits- und Gesundheitsschutz Pflichtveranstaltungen vorgeschrieben sind, gibt es bei der Unternehmenssicherheit nichts dergleichen.

Kritische Augen richten sich auf jede Sicherheitsrichtlinie. Es liegt an der Form der Unterweisungen, die normale Skepsis zurückzudrängen.
Foto: Sandra Nabbefeld / pixelio.de

Die Sensibilisierung der Mitarbeiter gelingt aber nur, wenn nicht nur der Verstand, sondern auch die Herzen erreicht werden. Denn eines steht unumstößlich fest: Sicherheit kann nur dann effektiv sein, wenn sie gelebt wird. Und gelebt wird nur etwas, von dem man überzeugt und durchdrungen ist, was man quasi als Teil seines eigenen Ichs akzeptiert hat.

Eine solche stabile Abwehrhaltung kann sich nicht auf Befehl von oben entwickeln. Sicherheit kann man zwar anordnen, aber dadurch wird sie zu einem Fremdkörper im Alltag der Menschen. Im Zuge einer „Befehlskette" werden Richtlinien und Policys nur halbherzig befolgt. Eine befohlene Sicherheit ist und bleibt etwas Aufgezwungenes, etwas, was „die da oben wollen". Etwas, dem man nur deshalb nachkommt, weil die Missachtung zu Sanktionen führt.

Die ärgsten Feinde einer solchen Sicherheitskultur sind Langeweile und unangemessene Platzierungen. Langweilige Vorträge sind ein lähmendes Gift für Aufmerksamkeit, Konzentration und Akzeptanz.

Wenn Sie das Thema als einen der Punkte unter vielen in eine Betriebsversammlung einbetten, signalisieren Sie dadurch bereits eine fragliche Wertigkeit. Wird der Tagesordnungspunkt dazu noch im letzten Viertel der Versammlung platziert, wenn viele Teilnehmer schon von den vielen Informationen übersättigt sind, ist die Gefahr groß, dass Sie weitestgehend ins Leere reden.

Beschäftigen wir uns kurz mit der menschlichen Psyche. Was passiert, wenn man von Menschen eine Änderung erwartet, die ja jede neue Sicherheitsmaßnahme bedeutet? Es gibt neben Gleichgültigkeit zwei widerstrebende Kräfte, die unser Innenleben bestimmen. Eine verleiht uns Elan und treibt uns vorwärts. Die andere, treffend auch „innerer Schweinehund" genannt, lässt uns in Aktionslosigkeit versinken. Man könnte sie mit Gaspedal und Bremse vergleichen. Wir bremsen, wenn wir unsicher sind und etwas nicht einsehen. Und wir geben Gas, wenn wir von einer Sache überzeugt sind und die noch aktiven inneren Widerstände auf Standby geschaltet werden.

Innere Widerstände sind etwas ganz Normales – etwas, das zum Menschsein dazugehört. Veränderungen rufen immer Gegenreaktionen hervor. Denn ein Mehr an Sicherheit bedeutet, dass Menschen sich verändern und neue Betrachtungsweisen und Blickwinkel annehmen müssen. Hinzu kommt, dass oft genug eine verbesserte Sicherheit mit einem kleinen oder

größeren Arbeitsaufwand verbunden ist. Ein Sicherheitschef formulierte es einmal so: „Sicherheit wird als unbequem empfunden". Denn man muss zweimal nachdenken. Einmal im Sinne des Arbeitserfolges und der Zielerfüllung, ein zweites Mal im Sinne der Sicherheit. Das erscheint vielen Menschen als lästig.

Vor allem dann, wenn der Sinn von Sicherheit nicht verstanden wird. Der „innere Schweinehund" ist es wiederum, der den Menschen zuflüstert: „Ist doch alles übertrieben. Wirtschaftsspionage, das ist mir zu viel James Bond. Alles Stoff fürs Kino, aber nicht für das wahre Leben."

So genannte Killerphrasen machen in solchen Situationen oft die Runde. Der Begriff Paranoia, eine schlimme psychische Erkrankung mit zwanghaften Wahnvorstellungen, wird dann bemüht, um Sicherheitsbemühungen in eine schiefe Ecke zu stellen und sie als Hysterie zu brandmarken.

Es gibt eine seltsame Neigung, Sicherheit selbst dann, wenn sie uns schützen kann, als etwas Einschränkendes, der Freiheit Entgegenstehendes, Kontrolle über uns Ausübendes zu betrachten. Das mag unter totalitären Regimen durchaus der Fall sein, ist aber in freiheitlich-demokratischen Gesellschaften grundsätzlich anders zu sehen. Möglicherweise ist diese Sichtweise den schwierigen Phasen der Geschichte geschuldet.

Eine von oben herab befohlene Sicherheit kann niemals das Niveau einer gelebten Sicherheit erreichen. Ein wichtiges Moment, die Mitarbeiter wirklich zu erreichen, ist Wertschätzung und Respekt. Foto: Gisela Peter / pixelio.de

Mit Vorträgen allein lässt sich keine tragfähige Sicherheitskultur aufbauen. Foto: Karl-Heinz Laube / pixelio.de

Gegenüber Sicherheitsbemühungen ist bei einem Teil der Menschen eine tendenziell ablehnende Haltung zu beobachten. Externe Berater können davon ein Lied singen. Anders als bei Firmenmitarbeitern oder Vorgesetzten, denen sie verbunden oder verpflichtet sind, offenbaren die Teilnehmer den Externen häufig, wie sie wirklich denken. Referenten von Inhouse-Schulungen, blicken oft in gelangweilte, desinteressierte Zuhörergesichter oder nehmen gar Zeichen einer offenen Antihaltung wahr. Da die Berater „von außen" meist einmal kommen und dann nie wieder, gibt sich das Publikum weniger Mühe, dienstbeflissen eine gute Miene aufzusetzen.

Behalten wir im Fokus: Der innere Widerstand ist eine Konstante, die da ist, auch wenn wir uns motiviert fühlen. Aber die Nein-Gestimmheit im Seelenleben kann entscheidend zurückgedrängt werden. Durch die Form, wie die Kampagne gestaltet wird und die das darin zu erkennende Engagement.

Wenn Sie sich zu einer Sensibilisierungskampagne entschließen oder einen Kunden dazu animieren möchten, denken Sie also an die äußere Form. Wichtig: Sie sollten den Punkt Sicherheit nicht mit anderen Themenfeldern verbinden. Wenn es überhaupt nicht anders geht, als die Schulung in eine Betriebsversammlung einzubetten, sollte dieser Tagesordnungspunkt auf jeden Fall im Anfangsbereich liegen und nicht am Ende, wenn Aufmerksamkeit und Konzentration bereits deutlich nachgelassen haben. Sonst ist die Gefahr groß, ins Leere zu reden.

Ungünstige Zeiten, um wichtige Inhalte zu vermitteln, sind die Stunden direkt vor oder nach der Mittagspause oder am Ende der Arbeitszeit. Denken Sie auch daran bei der Terminierung. Günstig sind Zeitpunkte zwischen 9 und 11 Uhr, am besten mit einer Kaffeepause.

Um zu verdeutlichen, dass das Thema Sicherheit nicht unter ferner liefen, rangiert, sollten Sie einen interessanten hochkarätigen Redner engagieren. Die IT-Sicherheitsproblematik könnte durch einen ethisch arbeitenden Hacker dargestellt werden. Behördenvertreter können anschaulich aus den Bereichen Wirtschaftsspionage und Mitarbeiterkriminalität berichten. Als Referenten denkbar wären auch geläuterte Ex-Täter. Ebenso sind Sicherheitsexperten anderer Unternehmen oder der Sicherheitsverbände eine gute Option. Gerne können auch Videoclips eingestreut werden – sie lockern ungemein auf. Die Inhalte dürfen nicht trocken dargeboten werden, sondern sollen spannend rüberkommen. Durch die besondere Art der Präsentation unterstreichen Sie, dass es sich um ein relevantes Thema handelt.

Es ist immer auch wichtig, wie sich der oberste Chef verhält. Ist er überhaupt bei der Veranstaltung dabei oder zeigt er bereits durch Nichtteilnahme, dass sein eigenes Interesse gering ist. Ein Sicherheitsberater berichtet, Chefs

hätten während der Veranstaltung in Akten gelesen oder nach wenigen Minuten den Raum verlassen. Dabei ist gerade das Chefverhalten von entscheidender Bedeutung. Es ist immer wieder zu beobachten, dass die Mitarbeiter sehr genau auf die Reaktionen der Chefs achten. Signalisiert die Unternehmensführung mangelndes Interesse oder glänzt sie durch Abwesenheit, werden auch die besten Referenten ihr Publikum nicht überzeugen können. Eine Veranstaltung dagegen, an der auch der Chef teilnimmt, gewinnt automatisch an Bedeutung.

Stellen Sie nicht nur das Unternehmen in seiner Gesamtheit in den Vordergrund, sondern beleuchten Sie immer auch welche Folgen sicherheitsschädliche Handlungen für den einzelnen Mitarbeiter hätten. Belegen Sie dies möglicherweise durch beispielshafte Zahlen. Es gibt eventuell auch in Ihrem Umkreis Unternehmen, die durch Datendiebstahl und andere kriminelle Handlungen derart geschädigt wurden, dass sie Personal abbauen oder sogar den Betrieb völlig einstellen mussten.

Zeigen Sie gegenüber den Mitarbeitern Respekt und Wertschätzung. Sprechen Sie möglichst nicht von der „Schwachstelle Mitarbeiter", sondern bestärken Sie die positiven Möglichkeiten, die in der Hand jedes einzelnen Mitarbeiters. Betonen Sie den Wert aller Beteiligten beim Sicherheitsbemühen.

Abwehrhaltungen, innere Widerstände. allem Neuen erst einmal skeptisch begegnen- das gehört nun einmal zum Menschsein dazu.
Foto: Axel Hopfmann / pixelio.de

Fakt ist: Richtig sensibilisiert stellen Mitarbeiter einen Verteidigungsring dar, der mindestens so wertvoll ist wie technikbasierte Abwehrmechanismen, und auf den niemand in Zeiten globaler Bedrohungen verzichten sollte. ←

Analysen und Hilfestellungen zum Wirtschaftsschutz

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

BSI-Notfallkarte für IT-Notfälle

→ Die Ende September 2019 vorgestellte sogenannte IT-Notfallkarte enthält Handlungsanweisungen für IT- bzw. Cyberangriffe. Die IT-Notfallkarte wird ergänzt durch einen Maßnahmenkatalog: Notfallmanagement und eine TOP12-Übersicht: Maßnahmen bei Cyberangriffen. **www.allianz-fuer-cybersicherheit.de** ←

Lagebild Wirtschaftsschutz NRW 2019

→ Erstmals wurde in NRW ein entsprechendes Lagebild erstellt, an dem sich allerdings nur 380 von insgesamt 20.000 angefragten Unternehmen beteiligten. Die Ergebnisse sind wenig überraschend. Je größer ein Unternehmen ist, desto umfassender ist es geschützt. Allerdings stehen die Unternehmen im Bereich Cybersicherheit besser da als beim Gebäudeschutz.

www.im.nrw ←

Kriminalitätsbarometer Berlin-Brandenburg 2019

→ In dieser von den IHK Berlin und Brandenburg seit 2005 durchgeführten deutschlandweit einzigartigen repräsentativen Dunkelfeldbefragung beteiligten sich 1.624 Unternehmen. Zwei Drittel der Unternehmen sind 2018 Opfer von Straftaten geworden. Am häufigsten waren die Unternehmen von Diebstählen (34 Prozent) bzw. Vandalismus (30,5 Prozent) betroffen. Stark gestiegen ist die Zahl der IT-Angriffe. Mehr als die Hälfte der Delikte werden nicht zur Anzeige gebracht. **www.ihk-berlin.de** ←

Bundeslagebild Organisierte Kriminalität 2018

→ Die Gesamtzahl der Ermittlungsverfahren gegen OK ist gegenüber 2017 um 6,5 Prozent gesunken. Der erfasste Schaden lag bei 691 Millionen Euro. Hauptbetätigungsfelder der OK blieben Rauschgiftkriminalität (37,6 Prozent), gefolgt von Eigentumskriminalität (17,4 Prozent) und Wirtschaftskriminalität (10,3 Prozent). **www.bka.de** ←

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Klaus 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