BEILAGE ZUM DSD 1 | 2018

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Es besteht eine akute Gefahr

Eine aktuelle Serie hat ein besonders brisantes Thema wieder in das Bewusstsein der Menschen gerückt: Brief- und Paketbomben. Bekanntermaßen wird DHL, ein Tochterunternehmen der Deutschen Post AG, von unbekannten Tätern erpresst. Es soll ein Millionenbetrag gezahlt werden, andernfalls würden weitere explosionsfähige Briefe und Pakete versandt. Nach Polizeiangaben besteht derzeit gerade für kleine und mittelständische Unternehmen, aber auch für Privatpersonen, eine akute Gefahr.

Die DHL-Serie ist besonders gefährlich, weil die Motive der Täter überhaupt nicht auf die Empfänger bezogen sind. Die Adressaten sind lediglich Mittel zum Zweck, um auf das erpresste Unternehmen Druck auszuüben. Das bedeutet: Jeder kann theoretisch zum Bombenziel werden – ohne dass ein ihn direkt betreffendes Motiv vorliegt.

Info Wirtschaftsschutz nimmt diese ernste Gefährdungslage zum Anlass, in dieser Ausgabe schwerpunktmäßig auf gefährliche Postsendungen einzugehen. Die einzig effektive Schutzmaßnahme im nicht-technischen Bereich ist und bleibt Vorsicht, Umsicht und Prävention. Die meisten Angriffe mit Brief- oder Paketbomben konnten verhindert werden, weil Mitarbeiter/innen mehr als nur einen flüchtigen Blick auf die relevanten Postsendungen geworfen haben. Acht- und Wachsamkeit sowie eine bewusste Abkehr von gefährlichen Routinen halfen zu verhindern, dass die Täter zum Ziel kamen.

Genauer hingucken, auf Besonderheiten achten, kompromisslos handeln im Verdachtsfall. Das sollte unser heutiges Credo sein.

Bleiben Sie also auch in dieser Hinsicht auf der sicheren Seite.

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz

Schlummernde Gefahr: Erst beim Öffnen eines Briefes bzw. eines Pakets wird in den meisten Fällen die Zündvorrichtung ausgelöst. Sorgfältige Kontrolle aber kann verhindern, dass es zum Schlimmsten kommt.
Foto: Lupo/pixelio.de

Pakete sind eine besondere Gefahr, denn sie können eine große Menge Sprengstoff enthalten. Bei solchen großformatigen Postsendungen sollte die interne Prüfung ganz besonders sorgfältig verlaufen.
Foto: Rainer Sturm/pixelio.de

Typische Warnsignale: Woran Brief- und Paketbomben im Vorfeld erkannt werden können

Von Klaus Henning Glitza

➔ Sie sehen fast so aus wie normale Postsendungen: Brief- und Paketbomben. Fast… denn wer genau hinsieht, kann möglicherweise verdächtige Merkmale entdecken. Und handeln bevor es zum Äußersten kommt. Denn Sprengstoff enthaltende Postsendungen werden nach Angaben von Polizei und DHL erst dann zur Bedrohung, „wenn sie aktiv geöffnet werden".

Die Gefahr, eine mit Explosivstoffen bestückte Sendung im Posteingang vorzufinden, ist derzeit nicht zu unterschätzen. Der Paketdienstleister DHL fordert deshalb zu besonderer Vorsicht auf: „Unseren Kunden empfehlen wir, vorerst nur Sendungen von bekannten Absendern anzunehmen oder Sendungen, die man selbst bestellt hat. Zudem hat das Unternehmen sowohl an Kunden wie an unsere Mitarbeiter folgende Anhaltspunkte für ein verdächtiges Paket oder eine verdächtige Briefsendung kommuniziert: Fehlender oder unvollständiger Absender, auffällige Rechtschreibfehler, Flecken oder Verfärbungen, Drähte oder andere Auffälligkeiten", so Dunja Kuhlmann, Pressesprecherin von DHL.

Die Grundbestandteile von Brief-/Paketbomben zu besorgen, bedarf keiner übermäßigen Anstrengung. Ein Beispiel dafür ist der Paketbombenfund von Potsdam. Als Sprengstoffquelle diente ein sogenannter „Polenböller". Das ist ein Feuerwerkskörper, der aufgrund seiner gefährlich erhöhten Explosivwirkung in Deutschland nicht erlaubt ist, aber in Ländern wie Polen problemlos und ganzjährig erhältlich. Zusätzlich war in der relevanten Postsendung eine Metalldose mit hunderten Nägeln enthalten, die eine verheerende Splitterwirkung entfaltet hätten.

Ein Indiz ist immer auch das Porto. Sind Briefmarken über das notwendige Maß hinaus aufgeklebt, sollte genauer hingeguckt werden.
Foto: Claudia Hautumm/pixelio.de

Aus Tätersicht sind Brief- und Paketbomben ein „attraktives" Tatmittel. Die gefährlichen Sendungen finden – sofern keine ordentliche Eingangspostkontrolle stattfindet – ihren Weg in gesicherte Bereiche, die auf physischem Wege kaum zu erreichen sind. In den Vereinigten Staaten sind mit Sprengstoffen bestückte Postsendungen bereits zum Massenphänomen geworden. In den zurückliegenden zehn Jahren registrierten US-Sicherheitsbehörden rund 10.000 Fälle – 80 Prozent davon mit kriminellen Hintergründen.

Ein wichtiges Warnsignal ist vor allem ein Missverhältnis zwischen Format und Gewicht der Sendung. Eine Brief-/Paketbombe besteht neben der Umhüllung meist aus drei Komponenten: Hauptladung (Sprengstoff), Zündvorrichtung und Energiequelle (Batterie oder Knopfzelle). Diese Grundbestandteile passen kaum in einen 20-Gramm-Standardbrief. Aus bisherigen Fällen ist bekannt, dass die explosionsfähigen Sendungen zwischen **vier bis sieben Millimeter dick waren und im Briefformat zwischen 40 und 70 Gramm wogen**. Päckchen/Pakete können natürlich deutlich schwerer sein. Ein weiteres Warnsignal ist eine offensichtliche Ungleichverteilung der Inhalte.

Schon ein paar Gramm Sprengstoff genügen, um Leib und Leben zu bedrohen. Problematisch ist dabei der geringe Abstand (maximal eine Armlänge) zwischen der explosionsfähigen Sendung und der Person, die sie öffnet. Neben der sich mit Überschallgeschwindigkeit ausbreitenden Stoßwelle und einer Stichflamme tritt bei einer Detonation enorme Hitze (bis zu mehrere 1.000 Grad) auf, die in der unmittelbaren Umgebung zu verheerenden Schäden führt.

Aus den USA wird berichtet, dass die Umhüllung von Sendungen mit explosivem Inhalt ungewöhnlich starr und fest wirkt. Ein weiteres Warnsignal ist, wenn die Sendungsinhalte ungewöhnlich elastisch sind oder sich wie Luftpolster anfühlen. Elastizität ist das Merkmal von plastischen Sprengstoffen.

Besonders gravierend sind die Erkennungszeichen, **wenn sie in Kombination auftreten**.

Klare Indizien sind:

» Ungewöhnlicher Geruch jeder Art.
» Schwacher Geruch nach Nitrolackverdünnung (Semtex) oder Mandeln/Marzipan (C4).
» Aus dem Brief ragen Drähte heraus oder beim Öffnen werden Drähte sichtbar.

- Aus einer beschädigten Sendung treten pulverförmige Substanzen oder Stoffe aus, die wie Fensterkitt aussehen.
- Übertrieben starke Sicherung der Sendung mit Klebeband.
- Verschnürungen oder Fäden (beide könnten mit Klebeband getarnt sein) führen ins Innere der Sendung.
- Beim Öffnen der äußeren Verpackung wird eine weitere Verpackung sichtbar, die besonders intensiv verklebt ist.

Verdächtige Anzeichen können auch bei den **Empfängerangaben** auftreten:

- Adressierung nicht am üblichen Platz (unten rechts).
- Es wird nur eine Funktionsbezeichnung ohne dazugehörigen Namen angegeben, z. B. „An den Geschäftsführer der Firma X".
- Rechtschreibfehler – Beispiel: Eine 1952 versandte Briefbombe war „An dem Bundeskanzler Dr. Konrad Adenauer" gerichtet und mit der fehlerhaften Ortsangabe „Frankfort" versehen. Absender war eine ausländische Terrororganisation.
- Zusätze wie „Persönlich-eigenhändig", „Nur vom Empfänger zu öffnen", „Vertraulich", die sicherstellen sollen, dass der angegebene Adressat die Sendung öffnet und geschädigt wird.

Bei den **Absenderangaben** sollte auf folgende Auffälligkeiten geachtet werden:

- Unleserliche Schreibweise.
- Trotz Firmenabsender handschriftlich verfasst.
- In ungelenk wirkenden Druckbuchstaben geschrieben, die den Zweck haben könnten, Charakteristika der Handschrift zu verdecken.
- Schablonenschrift.
- Stempel weist Hinweise auf, dass ein Stempelset/Kinderstempel benutzt wurde (nicht akkurate Ausrichtung der einzelnen Buchstaben, ungewöhnliche Schriftformate).
- Absenderadresse weicht vom Einlieferungsort ab oder
- ist offensichtlich ein Phantasieprodukt.

Auch ein **überhöhtes Porto** sollte Verdacht auslösen. Hintergrund könnte sein, dass der Absender die Zustellung unbedingt sicherstellen will, aber bei der Einlieferung nicht persönlich in Erscheinung treten will.

Eine der High-Tech-Lösungen für die technische Detektion von Brief- und Paketbomben: Der Millimeterwellenscanner T-Sense. Kleinere Unternehmen, die nicht zu solchen Optionen greifen wollen, sollten auf jeden Fall verdächtige Sendungen mit einem Metalldetektor überprüfen. Nachteil: Metalldetektoren sprechen auch auf Büro-und Heftklammern an. Foto: Hübner GmbH & Co. KG

Besteht der geringste Verdacht, sollten Plausibilitätsprüfungen und weitere Checks erfolgen: Entspricht die Adresse der behaupteten Person/Organisation?

Empfängerbezogen: Frage an den Empfänger, ob er die als Absender angegebene Person/Organisation/Institution kennt oder ob er von diesen eine Sendung erwartet.

Absenderbezogen: Rückfrage, ob die entsprechende Sendung an den Empfänger verschickt wurde und was sie enthält.

Entsprechen die **äußeren Charakteristika** der Sendung der Aufmachung, die vom Absender zu erwarten ist? Beispiel: Bei einem deutschen Unternehmen traf ein Brief mit der Absenderangabe „Europäische Zentralbank" ein, doch widersprachen die äußeren Merkmale der Sendung der Aufmachung, die bei einer solchen Institution vorauszusetzen sind.

Was tun in der Echtlage?

Unbedingt vorher festlegen und in einem Konzept verankern, was bei einem verdächtigen Fund geschehen soll.

Generell: Im Zweifelsfall die weitere Bearbeitung einer verdächtigen Sendung augenblicklich abbrechen, diese an Ort und Stelle liegen lassen und den Raum unverzüglich verlassen. Jedes An- oder Ausschalten von elektrischen Geräten oder der Beleuchtung vermeiden. Die Sendung niemals einer starken Lichtquelle aussetzen, auch nicht Fotokopier- und Blitzlichtgeräten. Dies könnte eine Zündvorrichtung (Lichtsensor) aktivieren. Der verdächtige Gegenstand muss auch von Feuchtigkeit ferngehalten werden (Kurzschlussgefahr!).

Unmittelbar nach Verlassen des Raums eine vorher festgelegte Stelle (Polizei über 110 sowie die verantwortliche Stelle im Unternehmen) verständigen. Die Sorge, dass die Kosten des Einsatzes in Rechnung gestellt werden, wenn sich die verdächtige Sendung als harmlos erweist, ist im Übrigen unbegründet. „Grundsätzlich dürfte ein im Nachhinein als ungefährlich bewerteter Gegenstand keine negativen Folgen für den Meldenden haben", teilt dazu Hans Retter, Pressesprecher des Landeskriminalamtes Niedersachsen, mit. Bei einer vorsätzlichen Falschmeldung hingegen müsse „mit entsprechenden Konsequenzen gerechnet werden, wie Auferlegung der verursachten Kosten und einer Strafanzeige wegen Störung des öffentlichen Friedens durch Androhung von Straftaten und/oder Missbrauch von Notrufen".

Wichtig: Die Meldung sollte ausschließlich über Festnetzgeräte (vorzugsweise im Nachbarraum) erfolgen, nicht über Schnurlos- oder Mobiltelefone beziehungsweise Funk. Kann nur ein Mobiltelefon genutzt werden, sollte der Abstand zum verdächtigen Fund 100 bis 200 Meter betragen.

Beschäftigte in den Nachbarräumen (auch in den darüber- und darunterliegen-

den Etagen und im unmittelbaren Außenbereich) müssen vorsorglich gewarnt werden. Das Gebäude sollte sodann evakuiert werden (Sammelplatz in sicherer Entfernung vorher festlegen und kommunizieren). Mobiltelefone und Funkgeräte müssen innerhalb eines kritischen Bereichs (100 bis 200 Meter) sofort ausgeschaltet werden.

Sollte **geschultes Sicherheitspersonal** mit einer potenziellen Brief-/Paketbombe konfrontiert werden, ist folgendes zu beachten: Die verdächtige Sendung hat die mechanischen Beanspruchungen des Postversands überstanden, ohne zu detonieren. Es kann folglich davon ausgegangen werden, dass sie nicht allein durch Bewegung zur Auslösung kommt. Trotzdem müssen grobmotorische Einwirkungen (hartes Abtasten, Knicken, Schütteln) unterlassen werden.

Generell ist es ratsam, wenn der Fund an einen Ort verbracht wird, wo er möglichst wenig Personen- und Sachschaden anrichten kann. Keine gute Idee ist es aber, den Gegenstand in einen kleinen fensterlosen Raum zu verbringen. Dort kann sich eine mögliche Detonation nicht verteilen, was die Explosivwirkung enorm erhöht. Auch sollten andere Räumlichkeiten im Inneren eines Gebäudes als Ablageorte gemieden werden. Am besten geeignet ist ein an der Gebäudeperipherie liegender Raum mit Außenfenstern.

Legen Sie die Sendung nicht in eine Kiste oder ein anderes verschließbares Behältnis. Dies stellt bei einer Detonation keinen Schutz dar, sondern wirkt wie eine Verdämmung, die die Bombe erst richtig gefährlich macht. Auch eine sogenannte Sprengstoffdecke sollte aus den genannten Gründen nicht auf den verdächtigen Gegenstand gelegt werden.

Ein verdächtiger Gegenstand sollte in der Mitte des Raumes abgelegt werden, am besten an einer frei zugänglichen Stelle auf den Boden. So haben Entschärfer die Möglichkeit, problemlos technische Hilfsmittel wie Manipulatoren oder andere Roboter einzusetzen. ←

Analysen und Hilfestellungen zum Wirtschaftsschutz

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

Ernst & Young – Studie zum Datenklau

→ Im Rahmen einer repräsentativen Befragung von 450 Führungskräften deutscher Unternehmen wurde festgestellt, dass 44 Prozent der Unternehmen in den letzten drei Jahren ausspioniert wurden. Das sind in etwa dreimal so viele wie noch vor zwei Jahren. Häufigste Angriffsart waren Hackerangriffe auf die EDV-Infrastruktur (74 Prozent). Damit hat sich die Zahl der entdeckten Cyberattacken gegenüber 2015 verdreifacht. Trotz dieses Anstiegs sehen sich 82 Prozent der befragten Unternehmen als ausreichend geschützt an. **www.ey.com** ←

NIFIS-Studie: IT-Sicherheit und Datenschutz 2017

→ Laut dieser Studie sollen die Ausgaben deutscher Unternehmen für IT- und Informationssicherheit in diesem Jahr um rund ein Drittel ansteigen. Langfristig erwarten bis 2025 von den befragten IT-Experten 44 Prozent ein um etwa ein Drittel höheres Investment für IT-Sicherheit, verglichen mit den bisherigen Ausgaben. **www.nifis.de** ←

BKA-Monitoringbericht: Social Engineering (SE)/CEO-Fraud

→ In diesem Bericht hat das BKA den aktuellen Forschungsstand zum Thema SE / CEO-Fraud der letzten fünf Jahre (2012-2017) zusammengestellt. Die Ergebnisse beruhen auf einer internetbasierten Literaturrecherche sowie auf einer Open-Source-Recherche. Im Bericht werden Studien, Fachartikel, ein laufendes Forschungsprojekt sowie Europol-Erkenntnisse zusammengefasst und bewertet. **www.wirtschaftsschutz.info** ←

DsiN/DIHK- Broschüre: IT-Dienstleistungen aber sicher!

→ Für eine sichere betriebliche IT-Infrastruktur ist die Auswahl des IT-Dienstleisters mitentscheidend. Der deutsche Mittelstand setzt bei der Auswahl von IT-Dienstleistern zum Betrieb und zur Wartung der IT-Systeme und zur Lösung aktueller Problemfälle überwiegend auf externe Dienstleister. Die DsiN/DIHK-Broschüre bietet Hilfestellungen und Empfehlungen für die Auswahlentscheidung. **www.sicher-im-netz.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