Handelsblatt

DEUTSCHLANDS WIRTSCHAFTS- UND FINANZZEITUNG

Verleger: Dieter von Holtzbrinck

Redaktion

Chefredakteur: Sven Afhüppe
Stv. d. Chefredakteurs: Sebastian Matthes (Head of Digital)
Stv. Chefredakteure: Peter Brors, Thomas Tuma

Autor: Hans-Jürgen Jakobs

Chefökonom: Prof. Dr. Dr. h. c. Bert Rürup

Leiter Digitales: Martin Dowideit

Chefreporterin: Tanja Kewes

Creative Director: Regina Baierl (Ltg.), Saskia Ballhausen (Stv. Ltg.)

Ressortleiter: Thomas Sigmund (Politik), Andrea Rexer (Unternehmen), Daniel Schäfer (Finanzen), Christian Rickens (Agenda), Nicole Bastian, Dr. Jens Münchrath (Ausland), Sönke Iwersen (Investigative Recherche)

Chef vom Dienst: Tobias Döring, Stefan Kaufmann, Marc Renner, Peter Pfister (News am Abend)

Deskchefs: Claus Baumann (Unternehmen), Julian Trauthig (Finanzen), Christoph Herwartz (Politik)

International Correspondents: Mathias Brüggmann, Torsten Riecke

Verantwortlich im Sinne des Presserechts sind die jeweiligen Leiter für ihren Bereich. Im Übrigen die Chefredaktion.

Handelsblatt Research Institute

Tel.: 0211 - 887-11 00, Telefax: 0211 - 887-97 11 00,
E-Mail: info@handelsblatt-research.com
Prof. Dr. Dr. h.c. Bert Rürup (Präsident),
Dr. Christian Sellmann (Managing Director)

Verlag

Handelsblatt GmbH (Verleger im Sinne des Presserechts).

Geschäftsführung: Frank Dopheide, Ingo Rieper, Gerrit Schumann

Anzeigenleitung: Andreas Wallenborn
Verantwortlich für Anzeigen: Peter Diesner

Erfüllungsort und Gerichtsstand: Düsseldorf.
Anschrift von Redaktion, Verlag und Anzeigenleitung: Toulouser Allee 27, D-40211 Düsseldorf, Tel. 0211 - 887–0
Der Verlag haftet nicht für unverlangt eingesandte Manuskripte, Unterlagen und Fotos.
Axel Springer SE, Offsetdruckerei Kettwig, Im Teelbruch 100, 45219 Essen; Pressedruck Potsdam GmbH, Friedrich-Engels-Str. 24, 14473 Potsdam; Süddeutscher Verlag Zeitungsdruck GmbH, Zamdorfer St. 40, 81677 München

Vertrieb Einzelverkauf:
Verlag Der Tagesspiegel GmbH, www.tagesspiegel.de

Kundenservice:
Postfach 103345, 40024 Düsseldorf,
Telefon: 0800 - 2233110,
Aus dem Ausland: 0049 211 887— 3602
E-Mail: kundenservice@handelsblatt.com
Ihre Daten werden zum Zweck der Zeitungszustellung übermittelt an Zustellpartner und an die Medienservice GmbH & Co. KG, Hellerhofstraße 2–4, 60327 Frankfurt am Main.

Anzeigen:
Anzeigenverkauf Handelsblatt
Tel.: 0211 - 887–24 84, Fax: 0211 - 887–33 59
E-Mail: info@iqm.de;
Internet: www.iqm.de
Anzeigenverkauf Handelsblatt.com
Tel.: 0211 - 887–26 26, Fax: 0211 - 887–97 26 56
E-Mail: info@iqdigital.de
Internet: www.iqdigital.de
Anzeigenverkauf Handelsblatt Personalanzeigen
Tel.: 040 - 32 80 229, Fax: 040 - 32 80 472
E-Mail: rosar@chancenundkarriere.de
Internet: www.chancenundkarriere.de
Anzeigendisposition Handelsblatt
Tel.: 0211 - 887 – 26 60, Fax: 0211 - 887 – 97 26 60
E-Mail: dispo.hb@iqm.de

Redaktion:
Telefax: 0211 - 887–97 12 40
E-Mail: handelsblatt@vhb.de
Politik
Tel.: 030 - 61 68 61 92, Fax: 0211 – 887–97 80 27
E-Mail: hb.berlin@vhb.de
Unternehmen
Tel.: 0211 - 8 87–13 65, Fax: 0211 - 8 87–97 12 40
E-Mail: hb.um@vhb.de
Finanzen
Tel.: 0211 - 887–4002, Fax: 0211 - 887–97 41 90
E-Mail: hb.fz@vhb.de
Agenda
Tel.: 0211 – 887–13 88, Fax: 0211 – 887–97 13 88
E-Mail: hb.agenda@vhb.de

Handelsblatt Veranstaltungen
Tel.: 0211 - 96 86 30 00, Fax: 0211 - 96 86 40 00
E-Mail: info@euroforum.com
www.handelsblatt.com/veranstaltungen

Artikelanfragen: Club-Mitglieder erhalten einen Artikel kostenlos, Telefon: 0800-2233110
E-Mail: artikelanfragen@vhb.de
Nutzungsrechte:
Telefon: +49 (0) 69/7591–29 30
(Dieser Service steht Ihnen Mo-Fr zu den üblichen Bürozeiten zur Verfügung) E-Mail: nutzungsrechte@vhb.de
Sonderdrucke:
Tel.: 0211 – 887–1748, Fax: 0211 – 887–97-1748
E-Mail: sonderdrucke@vhb.de

Bezugspreise Inland und EU:
monatlich € 66,70 (Inland inkl. € 4,36 MwSt./EU zzgl. der jeweiligen MwSt.). Jahresvorzugspreis: € 799,- (Inland inkl. € 52,27 MwSt./EU zzgl. der jeweiligen MwSt.). Vorzugspreis für Studenten (gegen Vorlage einer gültigen Bescheinigung): Monatlich € 33,30 (Inland inkl. € 2,18 MwSt. / EU zzgl. der jeweiligen MwSt.). Jahresvorzugspreis € 399,- (Inland inkl. € 26,10 MwSt. / EU zzgl. der jeweiligen MwSt.). Lieferung jeweils frei Haus. Bezugspreise übriges Ausland: auf Anfrage. Bezugspreise übriges Ausland: auf Anfrage.

Abonnementskündigungen sind nur schriftlich mit einer Frist von 21 Tagen zum Ende des berechneten Bezugszeitraumes möglich, solange keine andere Regelung vorgesehen ist. Im Falle höherer Gewalt (Streik oder Aussperrungen) besteht kein Belieferungs- oder Entschädigungsanspruch. Erfüllungsort und Gerichtsstand: Düsseldorf. Der Verlag haftet nicht für unverlangt eingesandte Manuskripte, Unterlagen und Fotos. Für die Übernahme von Artikeln in interne elektronische Pressespiegel erhalten Sie die erforderlichen Rechte über die PMG Presse-Monitor GmbH. Telefon: 030/284930 oder www.presse-monitor.de.
Die ISSN-Nummer für das Handelsblatt lautet: 0017–7296

Handelsblatt-Jahrestagung Cybersecurity

Der Feind in den eigenen Reihen

Die Abwehr von Hackern ist wichtig – aber was passiert, wenn die Mitarbeiter Daten stehlen? Der Mittelständler Compware Medical wäre daran fast zugrunde gegangen. Ein Lehrstück.

Lars-Marten Nagel Berlin

Von dem schrecklichen Verdacht hörte Gerd Meyer-Philippi (59) das erste Mal im Juli 2015 auf einer Konferenz in München. Eine Außendienstlerin erzählte dem Geschäftsführer des hessischen Mittelständlers Compware Medical eine wilde Geschichte. Ein freier Vertriebsmitarbeiter behauptete, er habe Maulwürfe in der Firma. Er wolle bald sein eigenes Ding machen. Meyer-Philippi glaubte das nicht. Er lachte.

Das ist ihm vergangen. Ein Apotheker, der eine Methadon-Abfüllanlage der Firma nutzte, fragte an, ob Compware Medical ein Datenleck habe. Ihm sei ein internes Protokoll eines Vier-Augen-Gesprächs vorgelegt worden. „Zunächst habe ich an Hacker gedacht“, sagt Meyer-Philippi. Aber schon bald gerieten mehrere seiner Mitarbeiter ins Visier.

Für die Firma begann eine Abwehrschlacht, die bis heute andauert. Es geht um die Reputation und die Existenz. „Die Jungs hätten uns das Genick brechen können“, sagt Meyer-Philippi. Die Anwaltskosten belaufen sich auf 250 000 Euro.

Der Fall von Compware Medical ist ein Beispiel dafür, wie häufig Unternehmen ihre Gefährdung falsch einschätzen. „Die Vorfälle anderer zeigen, dass unerlaubtes Verhalten vom Mitarbeiter bei der Betrachtung von Cybersecurity berücksichtigt werden muss“, sagt Thomas Schäfer, Chief Information Security Officer der Freudenberg-Gruppe, auf der Handelsblatt-Jahrestagung Cybersecurity am Dienstag in Berlin. Rund 120 Teilnehmer diskutieren zwei Tage die wichtigsten Entwicklungen in der IT-Sicherheit. Eine Erkenntnis: Bei jeder Risikobewertung müsse immer auch der böswillige Insider beachtet werden.

Der sogenannte „malicious insider“ ist auch ein Thema im Buch „Der Mensch als Risikofaktor bei Wirtschaftskriminalität“ der schweizerischen Wirtschaftsprüferin Sonja Stirnimann. Sie mahnt: „Es gibt weder kriminelle Computer noch kriminelle Codes.“ Wenn es darum gehe, wirtschaftskriminelle Ereignisse, Non-Compliance oder Cyberangriffe zu initiieren, abzuwehren und aufzuarbeiten, sei der Mensch das schwächste Glied in der Kette. Stirnimann: „Eine Existenzbedrohung kommt für normale Firmen selten von außen, sondern von Innentätern, die sehr lange dabei sind.“

> Eine Existenzbedrohung kommt für normale Firmen selten von außen, **sondern von Innentätern.**
>
> **Sonja Stirnimann**
> Wirtschaftsprüferin und Buchautorin

Die familiäre Atmosphäre war trügerisch

So war es auch im Fall Compware Medical. Die Firma ist einer der sprichwörtlichen Mittelständler, die gern als Rückgrat der deutschen Wirtschaft bezeichnet werden. Rund 40 Mitarbeiter erwirtschaften bis zu drei Millionen Euro Umsatz im Jahr. Sie konstruieren und warten Methadon-Dosiergeräte für Suchtambulanzen oder Justizvollzugsanstalten. Die Geräte sehen aus wie Kaffeeautomaten, stecken aber voller Hightech. Sie messen selbst die Verdunstung des flüssigen Methadons, denn der Umgang mit dem synthetischen Opioid erfordert maximale Präzision - so will es das Gesetz.

An der Wand in der Firmenzentrale in Gernsheim hängt eine Deutschlandkarte mit Steckfähnchen. Mehr als 280 Abfüllanlagen hat Compware Medical im Einsatz. Auch in Nepal, in

picture alliance / Ikon Images/T

Dietmar Gust

BSI-Präsident Arne Schönbohm: Eine Richtlinie für Router soll der Wirtschaft Orientierung geben.

Dietmar Gust

Podiumsdiskussion mit Arslan Brömme, Klaus Vitt, Thomas Schäfer und Tanja Lange: Mit der Komplexität der IT wächst auch das Risiko.

Malaysia und auf Mauritius gibt es die Geräte der Hessen. Das Team ist stolz darauf, dass täglich 20 000 Patienten mit seinen Automaten geholfen wird. Der Umgang untereinander ist locker. Die Chefs duzen sich mit allen. Freitags essen sie gemeinsam. Der Beagle einer Kollegin stromert über die Flure. Für seine Leute könne er die Hand ins Feuer legen, dachte Meyer-Philippi immer. Ein Trugschluss.

Das erste Notfalltreffen im Herbst 2015 blieb geheim. Nur die Geschäftsführung und der IT-Administrator diskutierten: Was tun mit dem bösen Verdacht? Der Administrator sagte: „Es werden auffällig große Datenmengen bewegt." Betroffen sei auch die Datei mit dem „Risikomanagement". Das Dokument sei die DNA des Unternehmens, sagt Meyer-Philippi. „Darin sind alle Risiken und ihre Bewertung aufgelistet, das gesamte Wissen der Firma, Konstruktions- und Softwarepläne, alle Stärken und Schwächen unserer Systeme." Die Runde beschloss, einen externen Forensiker einzuschalten und sonst Stillschweigen zu bewahren. Sie wollten die Täter in Aktion beobachten.

Der Forensiker schloss einen Hackerangriff schnell aus. „Das hat mich getroffen wie ein Hammerschlag", sagt Meyer-Philippi. Jetzt musste er Kollegen verdächtigen, und darauf war er nicht vorbereitet. Vier Personen gerieten ins Blickfeld: der Vertriebsmann, seine Frau, die auch im Unternehmen arbeitete, der Produktmanager Michael Dohmke (*), der bald ausscheiden wollte, und ein ehemaliger Auszubildender.

Die Ergebnisse des Forensikers seien eindeutig gewesen, sagt Meyer-Philippi. „Wir haben Chats rekonstruieren können, in denen sie sich austauschten." Der Chef ging zum Gegenangriff über, stellte die Zusammenarbeit mit dem Vertriebler ein. Im Dezember knallte es: Compware Medical kündigte die drei Verträge der Mitarbeiter fristlos und stellte eine Strafanzeige.

Mit der Trennung vom verdächtigten Personal waren für Meyer-Philippi die Sorgen nicht vorbei. Zwar begann die Staatsanwaltschaft zu ermitteln, aber vor dem Arbeitsgericht musste er einem Vergleich zustimmen, weil er aus taktischen Gründen nicht alle Fakten auf den Tisch legen wollte. Immerhin von der Arbeit der Behörden ist Meyer-Philippi beeindruckt. „Es dauert zwar alles ein wenig, aber die Polizei hat einen guten Job gemacht."

Noch während ihrer Tätigkeit bei Compware Medical verbündeten sich Michael Dohmke und der Ex-Azubi mit dem Ex-Vertriebsmann in einer neuen Firma. Deren Zweck: Entwicklung und Vertrieb medizintechnischer Geräte für Opiatabhängige. Meyer-Philippi hörte bald von Kunden, dass die neue Firma mit Niedrigstpreisen warb. „Sie haben vermutlich unsere Kunden durchtelefoniert, die Daten lagen dem Ex-Vertriebler natürlich vor", sagt der Geschäftsführer. Die Kundenkartei sei ein Vermögen wert, Methadonärzte finden sich nicht im Internet, die Kontakte wurden in mühseliger Kleinarbeit über Jahre gesammelt.

Immerhin: Der mutmaßlich illegal arbeitende Konkurrent aus den eigenen Reihen wurde langsamer. Vielleicht lag es an den Hausdurchsuchungen der Staatsanwaltschaft, die bald folgten. Vielleicht gingen die Pläne des Ex-Vertriebsmanns nicht auf. Das neue Dosiersystem der Ex-Kollegen ließ jedenfalls auf sich warten und kam erst Anfang 2017 auf den Markt.

Zu diesem Zeitpunkt galt der Ex-Vertriebsmann bei Meyer-Philippi und seinen Anwälten als Kopf der Verschwörer. Auf seinem Rechner hatten Polizisten die Kronjuwelen von Compware Medical gefunden, das Risikomanagement. Der Mann kann sich heute nicht mehr rechtfertigen, er ist verstorben.

Die Ermittlungen belasten dafür Ex-Produktmanager Dohmke schwer. Er ist nach dem Tod des Vertriebsmannes zum Geschäftsführer der Konkurrenzfirma aufgestiegen. Die Kripo aus dem Polizeipräsidium Südhessen hat sich festgelegt. Nur Dohmke könne das Risikomanagement kopiert und mitgenommen haben.

Der Beschuldigte bestreitet die Vorwürfe. Dohmke sieht sich als Opfer einer Intrige. Seine Version: Der Platzhirsch am Markt wolle einen lästigen, aber legal operierenden Konkurrenten loswerden. In einer Stellungnahme Ende August gab sich sein Anwalt kämpferisch: Er verglich den Vorwurf der Verletzung des Betriebsgeheimnisses mit einem schlecht gebauten Kartenhaus. Dohmke beharrt darauf, der neue Dosier-Apparat sei eine Eigenentwicklung. Laut Staatsanwaltschaft dauern die Ermittlungen an.

Patentanmeldungen vor vielen Jahren versäumt

Das hemmt die Geschäftsentwicklung. Die Firma der Ex-Mitarbeiter von Compware Medical residiert heute an der Wohnanschrift von Dohmke, der Umsatz lag 2017 bei weniger als 150 000 Euro. Für Meyer-Philippi hat die Phase der Aufarbeitung begonnen. „Was hätte ich merken müssen, und soll ich nun allen Mitarbeitern misstrauen?", fragt sich der Chef. Einen Fehler hat er bei sich selbst entdeckt. Er liegt Jahrzehnte zurück, wirkt aber noch immer nach: Es fehlt ein Patent. „Wir waren jung, und wir hatten einen tollen Auftrag", sagt Meyer-Philippi. „An Patentanmeldungen dachten wir nicht."

Drei wesentliche Faktoren bestimmten darüber, ob Menschen wirtschaftskriminell werden, sagt Expertin Stirnimann. Die Fachliteratur nennt es „Fraud-Triangle". Dazu gehören eine Gelegenheit, eine besondere Drucksituation, die oft auch im Privatleben des Täters zu suchen ist, und eine Rechtfertigung. „Es gibt immer Frühwarnindikatoren", sagt Stirnimann, leider erkenne man diese oft erst hinterher, weil die grundlegende Sensibilisierung dafür fehle.

Auch Meyer-Philippi sieht Ereignisse der Vergangenheit heute mit anderen Augen. Hätte es ihm auffallen müssen, als Dohmke sein geliebtes Motorrad verkaufte, möglicherweise wegen Geldsorgen? Und dass es dem Mann zusetzte, als die Firma sein Aufgabengebiet neu zuschnitt, weil er überfordert wirkte?

Welche technischen Standards die Sicherheit erhöhen, ist das Thema auf der Handelsblatt Cybersecurity-Tagung. Thomas Schäfer von der Freudenberg-Gruppe sagt, Firmen könnten viel tun, um es internen und externen Tätern schwerzumachen: „Der überlegte Umgang mit externen Schnittstellen an den Computern und der Einsatz von Verschlüsselung gehören dazu, ebenso ein vernünftiges Zugriffsmanagement und ein Logging und Monitoring der Zugriffe auf besonders sensitive Datenbestände."

Compware Medical habe die EDV-Struktur verändert, sagt Meyer-Philippi, Zugriffsrechte begrenzt und ein neues Sicherheitskonzept aufgesetzt. „Heute müssen Kollegen oft wegen Kleinigkeiten mit dem Administrator Rücksprache halten." Trotzdem könne die Firma den Zugriff auf das Risikomanagement nicht auf null begrenzen. Philippi hat sich fest vorgenommen, nicht jeden Mitarbeiter unter Generalverdacht zu stellen. Seinen Blick für die Kollegen, ihren Alltag und ihre Sorgen will er trotzdem schärfen. (*) Name geändert

Die Tagung

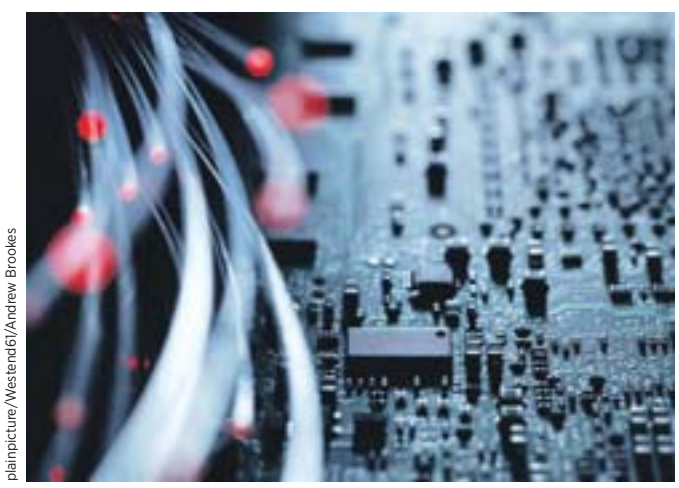
Das Publikum Mit der fortschreitenden Digitalisierung steigt auch das Risiko für Cyberangriffe. Auf der 8. Handelsblatt-Jahrestagung Cybersecurity in Berlin tauschen sich rund 150 Fachleute aus Unternehmen und Behörden aus.

Die Themen Die Vorträge beschäftigen sich mit einer großen Bandbreite von Themen, von der Datenschutzgrundverordnung über die Absicherung von Fabriken bis zur außenpolitischen Rolle der IT-Sicherheit.

CompWare Medical

Gerd Meyer-Philippi: Opfer böswilliger Insider.

Innenleben eines PC: Gefährliche Internetanbindung per Router.



plainpicture/Westend61/Andrew Brookes

Router

Sicherheit als Feature

Als im November 2016 die Router von mehr als einer Million Telekom-Kunden ausfielen, war das ein Weckruf für die deutsche Politik. Der Hackerangriff, der Telefon, Internet und teilweise auch das Fernsehen lahmlegte, zeigte die Verwundbarkeit der digitalen Infrastruktur.

Geht es nach Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), wird so etwas in Zukunft nicht so einfach wieder passieren können. Eine technische Richtlinie, vor zwei Wochen veröffentlicht, definiert Mindestanforderungen für die IT-Sicherheit bei Routern.

Es gebe nun „Leitplanken, an denen sich die Wirtschaft orientieren kann", sagte der Behördenchef am Dienstag auf der Handelsblatt-Tagung Cybersecurity in Berlin. Verbraucher könnten künftig erkennen, wie sicher diese Produkte seien - und Sicherheit als Mehrwert „einpreisen".

Die Hersteller sind nicht verpflichtet, die Richtlinie einzuhalten - nach Einschätzung des Innenministeriums müsste es dafür eine einheitliche Regelung innerhalb der EU geben. Schönbohm hofft aber, dass die Kennzeichnung zu einem Wettbewerb führt.

Zudem erwartet der BSI-Chef eine indirekte Wirkung über die Produkthaftung: Wenn Gerichte über solche Fälle entscheiden, berücksichtigen sie den Stand der Technik - der sei mit der Richtlinie dokumentiert: „Dadurch haben wir einen anderen Hebel."

Die Richtlinie hält Unternehmen an, schwere Sicherheitslücken durch Updates zu schließen. Zudem sollen sie transparent machen, wie lange die Geräte aktuelle Software erhalten. Wer die Vorgaben einhält, darf das durch eine Kennzeichnung am Gerät zeigen.

Der Chaos Computer Club (CCC) kritisiert, dass Verbraucher keine genaue Information erhalten, wie lange es Softwareupdates geben soll. Schönbohm hält dem entgegen, dass ein QR-Code am Gerät zu einer Webseite führt, die genaue Informationen zur Wartung nennt.

Die Kennzeichen dürften auch an Geräten fürs vernetzte Zuhause kleben. Das Bundesinnenministerium werde mit dem BSI, der Wirtschaft und Verbrauchervertretern Mindestanforderungen fürs sogenannte Internet der Dinge erarbeiten, kündigte Staatssekretär Klaus Vitt an.

Christof Kerkmann, Lars Nagel