Erfolgsfaktor IT-Sicherheit.

Vom Mittelstand für den Mittelstand.

[m] IT SICHERHEIT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

BVMW
Bundesverband
mittelständische Wirtschaft

www.bvmw.de

Stand: Februar 2013

Titelfoto: Pavel Ignatov/shutterstock.com

Grafik / Layout: Frithjof Siebert

Grußwort

Mario Ohoven ist Präsident des Bundesverbands mittelständische Wirtschaft (BVMW); er steht zugleich an der Spitze des europäischen Mittelstandsdachverbands (CEA-PME) in Brüssel. Foto: Silke Borek

Sehr geehrte Damen und Herren,

innovative digitale Lösungen bieten dem Mittelstand neue Wachstumsimpulse und Entwicklungschancen. Für kleine und mittlere Unternehmen (KMU) gehört der Einsatz von Informationstechnologien (IT) zum Geschäftsalltag: Zahlreiche, zum Teil vertrauliche Daten, werden über IT verarbeitet. Gleichzeitig haben zwei von drei deutschen Unternehmen in den vergangenen Jahren Daten verloren und dadurch wirtschaftlichen Schaden erlitten. Grund dafür ist oft ein fehlendes Bewusstsein für die Bedeutung sicherer IT-Systeme. IT-Sicherheit ist eine Grundvoraussetzung für unternehmerischen Erfolg und somit für den BVMW ein zentrales Anliegen.

Das vom Bundesministerium für Wirtschaft und Technologie im Rahmen der „Task-Force IT-Sicherheit“ geförderte Projekt „Bewusstseinsbildung für IT-Sicherheit in KMU – BVMW und Finanzierer als Brückenbauer“ setzt an dieser Stelle an.

Der BVMW hat hierzu eine Reihe von Initiativen und Aktionen gestartet. Einen ausführlichen Überblick über das Projekt finden Sie auch auf unserer Website www.mit-sicherheit.bvmw.de

Ihr

Mario Ohoven

Erfolgsfaktor [m]IT Sicherheit

Das Thema IT-Sicherheit im Mittelstand ist so aktuell wie nie zuvor. Als Innovationsmotor Deutschlands ist der Mittelstand beliebtes Opfer von Industriespionage. Personenbezogene Daten zu verkaufen, ist für Kriminelle hoch lukrativ. Fällt die IT auf Grund von Hard- oder Softwareproblemen aus, sind ganze Unternehmen nicht mehr arbeitsfähig. Dennoch ist die Investitionsbereitschaft häufig zu schwach ausgeprägt. Die Gründe sind vielschichtig. Die Kosten werden als zu hoch erachtet und die möglichen Schadenssummen ausgeblendet.

Diese Broschüre informiert über Gefahrenpotenziale für IT-Systeme und soll den Leser anhand von Beispielen aus der Praxis mit realen Schadenssummen für mehr IT-Sicherheit sensibilisieren. Sie wurde im Rahmen des von der Task Force „IT-Sicherheit in der Wirtschaft“ geförderten Projekts [m]IT Sicherheit mit Experten aus Mitgliedsunternehmen des BVMW erstellt. Die verwendeten Beispiele sind anonymisiert und wurden von den Teilnehmern der Expertengruppe zusammengestellt. Diese waren im Rahmen ihrer Tätigkeiten für die Eindämmung und Behebung der Schäden zuständig.

Der BVMW setzt sich auf allen politischen Ebenen für die Belange des Mittelstands in Deutschland ein. Das Projekt [m]IT Sicherheit trägt der zunehmenden Nutzung und damit wachsenden Abhängigkeit von IT-Anwendungen in Unternehmen Rechnung. Gemeinsam mit Finanzierern engagiert sich der BVMW im Projekt als Brückenbauer zu den Unternehmen. Laut einer aktuellen Studie[1] haben 99 Prozent der befragten KMU eine „IT-Grundausstattung“. Bereits 93 Prozent hatten Schadensfälle durch IT-bezogene Sicherheitslücken; 63 Prozent dieser Schadensfälle haben menschliches Fehlverhalten als Ursache. Die Schadenshöhe reichte von Kleinstbeträgen bis in die Millionen und führte in einigen Fällen unmittelbar in die Insolvenz.

Task Force „IT-Sicherheit in der Wirtschaft“

Die Task Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Technologie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind abrufbar unter: www.it-sicherheit-in-der-wirtschaft.de.

1 Studie „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen“ im Auftrag des Bundesministeriums für Wirtschaft und Technologie, September 2012. Link: http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

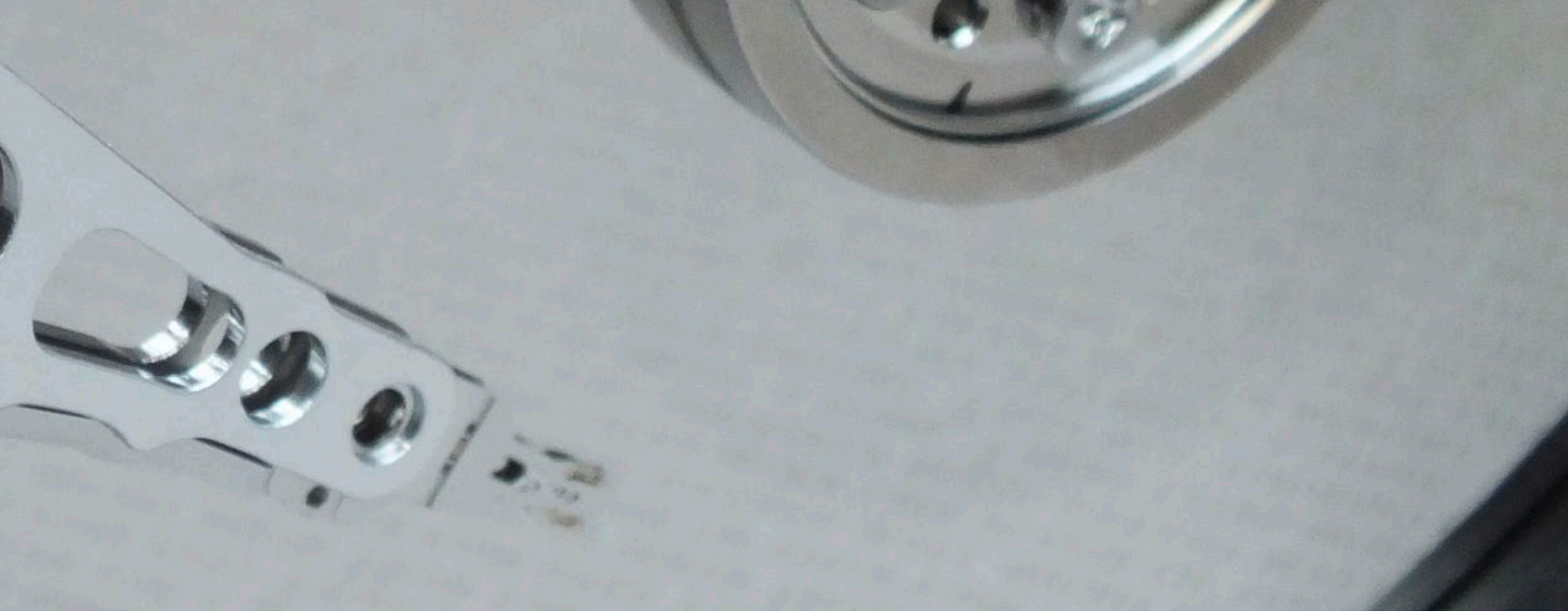


Bild: Th. Reinhardt / pixelio.de

Inhalt

Sicherheitsbereich:	**Redundante Systeme – Störung der Internetleitung**
Unternehmensart:	**Dienstleistendes Unternehmen (B2B/B2C)**
Unternehmensgröße:	**Bis 300 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**ca. 40.000 Euro**

Tag des Vorfalls

Bei einem Berliner Webunternehmen fiel vor wenigen Monaten die Internetleitung aus. Da alle 300 Mitarbeiter größtenteils mit Cloud-Lösungen arbeiteten, war das Unternehmen auf eine dauerhafte Internetverbindung angewiesen. Selbst die komplette Kundenbetreuung des Unternehmens arbeitete mit IP-Telefonen und einer gehosteten Telefonanlage. Somit waren durch die Störung der Internetleitung nicht einmal eingehende und ausgehende Telefonate möglich. Die Kunden des Onlineshops hatten keine Möglichkeit, das Unternehmen zu erreichen.

Bild: Benjamin Thorn / pixelio.de

Folgen

Durch die Störung der Internetleitung waren 300 Mitarbeiter arbeitsunfähig. Nach ca. 2 Stunden wurde der Großteil von ihnen nach Hause geschickt. Die Arbeit im Büro kam vollständig zum Erliegen, die unmittelbaren Schäden durch den Personalausfall betrugen ca. 40.000 Euro. Da das Unternehmen telefonisch nicht erreichbar war, erlitt es einen immensen Imageverlust. Potenzielle Kunden konnten keine Rückfragen zu den Produkten stellen. Die Probleme verbreiteten sich sehr schnell über diverse soziale Medien.

Lösung/Ergebnis

Als sofortige Lösung arbeiteten einige Mitarbeiter über UMTS Sticks. Schließlich gab es die Möglichkeit, ein Kabel über den Flur zu verlegen und sich auf die Internetleitung des Nachbarn im gleichen Gebäude aufzuschalten.

Prävention

Moderne Firewallsysteme ermöglichen die Bündelung mehrerer externer Internetanschlüsse. Durch die Zusammenschaltung mehrerer Internetzugänge erhält man eine Redundanz, so dass einzelne Anschlüsse ausfallen können, ohne dass der Betrieb gestört wird. Um sich vor dem Ausfall einer Firewall zu schützen, kann man zwei oder mehrere Firewalls zu einem Cluster zusammenschalten. Der Ausfall einer Firewall ist in diesem Aufbau unkritisch.

Expertentipp

Bündeln Sie Anschlüsse unterschiedlicher Anbieter basierend auf unterschiedlichen Übertragungsmedien. Eine Kombination von Anschlüssen über Glasfaser, Kupferleitungen und dem Fernsehkabel sorgt für beinahe absolute Ausfallsicherheit. Auch Kleinstunternehmen können sich den „Luxus“ redundanter Internetzugänge leisten. Kleine Firewallsysteme sind bereits für wenige hundert Euro erhältlich. Eine Kombination von einem VDSL Anschluss und einem Anschluss über das Kabelfernsehen ist extrem ausfallsicher und kostet monatlich weniger als 100 Euro. Entscheiden Sie sich am besten für mindestens einen Business-Tarif. Somit haben Sie die Möglichkeit, feste IP-Adressen zu nutzen, erhalten vertraglich garantierte Entstörzeiten, und der Anbieter ist bei längeren Ausfallzeiten haftbar für den entstandenen Schaden.

Sicherheitsbereich:	**Redundante Systeme – Ausfall des Raid Controllers**
Unternehmensart:	**B2C**
Unternehmensgröße:	**bis 50 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**mehrere 10.000 Euro**

Tag des Vorfalls

An einem Freitagabend gegen 22:00 Uhr fiel den Mitarbeitern der Nachtschicht auf, dass der Zugriff auf die zentrale Datenbank der Firma verweigert wurde. Die Administration wurde umgehend über einen vermeintlichen Serverausfall informiert. Der Techniker versuchte zunächst das Problem über eine Remote-Verbindung zu lösen. Jedoch war auch so keine Kommunikation mit dem Server möglich. Der Techniker begab sich sofort zur Firma. Nach eingehender Prüfung stellte er fest, dass es sich hierbei nicht um einen Serverausfall handelt, sondern dass das Storage-System betroffen ist. Der Raid Controller (Redundant Array of Independent Disks – Redundante Anordnung unabhängiger Festplatten) war durch einen Defekt ausgefallen.

Folgen

Da das System nicht abgesichert war, und die benötigten Ersatzteile auf Grund des Wochenendes nicht beschafft werden konnten, gelang eine kurzfristige Wiederherstellung des Systems durch den Techniker nicht. Durch den unvorhergesehenen Ausfall waren nicht nur die Mitarbeiter der Hauptniederlassung in Berlin, sondern auch zwei weitere Standorte des Unternehmens betroffen. Durch den Systemausfall konnten rund 50 Mitarbeiter über mehrere Tage nicht auf wichtige Informationen, Systembestandteile und Dokumente zugreifen. Die Geschäftsführung schätzt, dass ein unmittelbarer finanzieller Schaden in Höhe von mehreren 10.000 Euro entstanden ist.

Bild: Joerg Trampert / pixelio.de

Lösung/Ergebnis

Nachdem die notwendige Hardware geliefert wurde, war eine vollkommene Wiederherstellung des Systems möglich. Der entstandene Schaden konnte dadurch jedoch nicht mehr reduziert werden.

Prävention

Durch die Etablierung eines Redundanten Systems hätte der Schaden durch den Ausfall auf ein Minimum reduziert werden können. Die Mitarbeiter wären schon nach kurzer Zeit wieder in der Lage gewesen, ihre Arbeit aufzunehmen oder hätten den Schaden gar nicht bemerkt. Der erhebliche wirtschaftliche Schaden wäre komplett vermieden worden. Die nötigen Investitionen in ein Redundantes System verursachen Kosten in Höhe von ungefähr 8.000 Euro. Das Unternehmen ist in diesem Fall für einen Zeitraum von fünf Jahren vor einem solchen Ausfall und einem möglichen Datenverlust geschützt.

Expertentipp

Eine Redundanz, die nicht nur auf Festplattenebene (Raid) sondern auch auf Systemebene etabliert worden wäre, hätte den Ausfall verhindert. Ein solches redundantes System, dass auch die Serverebene mit einschließt und die Lastverteilung regelt, lohnt sich aufgrund seiner Funktionalitäten für jeden Betrieb, der viele Daten zu verarbeiten hat. Durch die Verteilung der anfallenden Last kann das System ohne Unterbrechung weiter arbeiten.

Sicherheitsbereich:	**Telefonie – Störung der Leitung**
Unternehmensart:	**Dienstleistendes Unternehmen (B2B/B2C)**
Unternehmensgröße:	**Bis 500 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**1.000 bis 30.000 Euro**

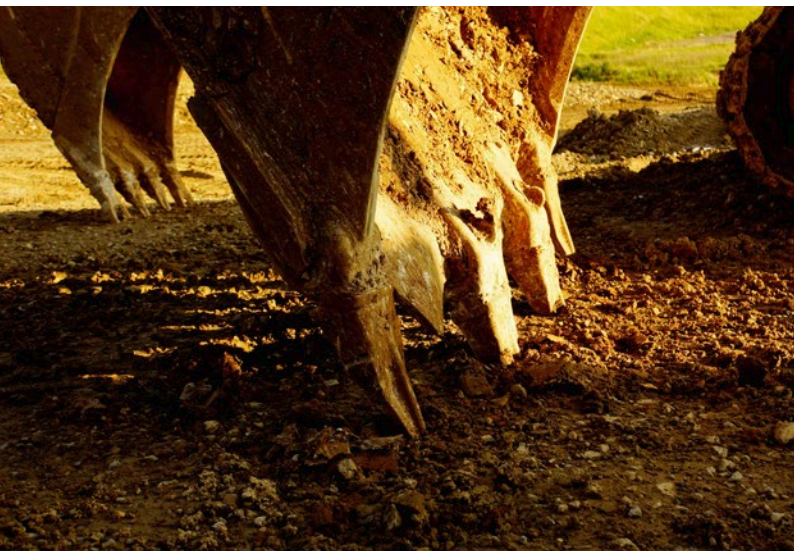


Bild: Rainer Sturm / pixelio.de

Tag des Vorfalls

Anfang des Jahres war das komplette Hamburger Büro eines mittelständischen Unternehmens, 200 Mitarbeiter an sieben Standorten in Deutschland, telefonisch nicht mehr erreichbar. Weder eingehende noch ausgehende Gespräche waren möglich. Bei Baumaßnahmen in der Nachbarschaft traf ein Bagger einige, für die Telefonie notwendige Kupferleitungen. Am Standort arbeiteten 30 Mitarbeiter. Da die Störung vier Tage andauerte, wäre dem betroffenen Unternehmen ohne eine schnelle Lösung ein erheblicher Schaden entstanden. Die Mitarbeiter wären nicht arbeitsfähig gewesen. Durch die fehlende Erreichbarkeit hätte darüber hinaus das Image des Unternehmens gelitten. In diesem Fall konnte eine Alternativlösung implementiert werden, mit der das Problem bis zur Entstörung durch den Provider gelöst wurde. Die Standorte des Unternehmens waren über ein verschlüsseltes Datennetz miteinander verbunden. Dies diente zum Datenaustausch und zur Verbindung der Telefonanlagen des Unternehmens untereinander. Die Vernetzung der Telefonanlagen war ursprünglich für Komfortfunktionen gedacht.

Folgen

Durch die Beschädigung der Leitung war das Unternehmen kurzfristig nicht erreichbar. Eine Alternativlösung führte dazu, dass der betroffene Standort statt vier Tagen lediglich eine Stunde nicht erreichbar war. Ein langfristiger Arbeitsausfall der Mitarbeiter hätte Personalkosten in Höhe von ca. 30.000 Euro sowie massive Imageschäden verursacht. Durch die schnelle Reaktion betrugen die unmittelbaren Kosten ca. 1.000 Euro.

Lösung/Ergebnis

Um das Unternehmen schnell wieder arbeitsfähig zu bekommen, wurde die Vernetzung der Telefonanlagen umfunktioniert. Alle ausgehenden Gespräche der Hamburger Mitarbeiter wurden über das Datennetz nach Berlin geleitet und dort über die Berliner Telefonanlage in das Telefonnetz eingespeist. Alle eingehenden Gespräche wurden durch den Telefonanbieter auf die Berliner Anlage weitergeleitet, so dass diese von dort aus auf die Hamburger Telefone gesendet werden konnten.

Prävention

Um den Ausfall einer Telefonanlage zu vermeiden, lassen sich moderne Anlagen zu einem Cluster bestehend aus zwei oder mehr Anlagen verbinden. Notfallpläne für den Ausfall der Telefonleitungen sorgen im Ernstfall für eine schnelle und strukturierte Problemlösung.

Expertentipp

Im Bereich der Telefonie existieren drei verschiedene Sicherheitsrisiken:

- Vertraulichkeit: unverschlüsselte Gespräche – insbesondere bei IP-Telefonie – können mitgehört werden;
- Integrität: Rufnummern können gefälscht werden;
- Verfügbarkeit: Telefonielösungen können ausfallen.

Diese Risiken sollten, genau wie alle anderen Sicherheitsrisiken, bewertet werden bevor ein Schaden eintritt, so dass gegebenenfalls Gegenmaßnahmen eingeleitet werden können.

Sicherheitsbereich:	**Mitarbeiter – Datendiebstahl**
Unternehmensart:	**Produzierendes Unternehmen (B2B)**
Unternehmensgröße:	**Bis 500 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**mehrere 100.000 Euro**

Tag des Vorfalls

Ein Unternehmen der Automobilzulieferindustrie entwickelt Maschinenwerkzeuge zur Herstellung von Karosserieteilen. Pläne und Studien zu diesem Projekt sind Teil der Betriebsgeheimnisse. In diesem Fall wurden die sensiblen Daten nicht nur von einem Mitarbeiter über USB-Stick entwendet, sondern auch gleich beim neuen Arbeitgeber, der in derselben Branche tätig ist, eingebracht.

Folgen

Das betroffene Unternehmen verlor kurzfristig einen Mitarbeiter, ohne dass zunächst weitere Schäden oder das unerlaubte Kopieren der Daten bemerkt wurden. Dass gemeinsam mit dem Mitarbeiter auch Daten verschwunden waren, stellte sich heraus, als ein sicher geglaubter Auftrag über mehrere 100.000 Euro an die Konkurrenz vergeben wurde.

Lösung/Ergebnis

Der Schaden für das Unternehmen ist irreparabel, eine Schadensbegrenzung nicht mehr möglich. Juristisch kann ein solcher Fall nur dann aufgearbeitet werden, wenn der Datendiebstahl durch entsprechende Protokolle bewiesen werden kann und/oder die Angestelltenverträge und Datenschutzvereinbarungen juristisch relevante Klauseln enthalten.

Prävention

Entsprechende Formulare, um notwendige Datenschutzvereinbarungen sowie Arbeits- und Prozessrichtlinien mit den Mitarbeitern zu vereinbaren, existieren bereits und können auf den individuellen Bedarf abgestimmt werden. Über Endpoint Protection Software, die neben Virenschutz, Web-Security und -Filtering, auch Client Firewall, Patch-Analyse und Application-Control bietet, können die Arbeitsplätze abgesichert und Datenübertragungen nach innen und außen kontrolliert werden. Über die Network Access Control werden Computer, die auf das Netzwerk zugreifen, überprüft, um die lückenlose Einhaltung von Richtlinien und Vereinbarungen zu gewährleisten. Mit einer integrierten Device Control können die Risiken für Datenverluste und Malwareinfektionen eingedämmt werden, indem Wechselmedien wie USB-Sticks, Laufwerke und Wireless Networking-Geräte (Bluetooth) kontrolliert und/oder blockiert werden. Zusätzlich werden über Data Control sensible Daten permanent gescannt. Da diese Scans in den Ablauf der Antiviren-Agenten integriert sind, kosten sie keine Systemperformance. Das gesamte Sicherheitsmanagement kann über eine zentrale Konsole gesteuert werden und verursacht Kosten in Höhe von 40 Euro/p.A. pro User-Neulizenz.

Expertentipp

Die Investition in Datenschutzvereinbarungen für Mitarbeiter sowie in die entsprechende Software zur Überprüfung der Einhaltung ist für jedes Unternehmen, das von Industriespionage bedroht ist, unbedingt notwendig. Die entstehenden Kosten sind unverhältnismäßig gering im Vergleich zum potenziellen Schaden. Außerdem rechtfertigen in den meisten Fällen die Zeit- und Kosteneinsparungen durch neue Software deren Preis. Häufig gibt es zu den Software-Lizenzen kostenfreie Sicherheitsupdates und Software-Upgrades, so dass Aktualität gewährleistet und Folgekosten überschaubar bleiben.

Sicherheitsbereich:	**Server – Ausfall durch eine defekte Platine**
Unternehmensart:	**B2B**
Unternehmensgröße:	**bis 100 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**über 70.000 Euro**

Tag des Vorfalls

In einem Unternehmen fiel der Datenserver durch eine defekte Platine aus. Der Server war fünf Jahre alt, so dass eine Ersatzplatine erst angefordert werden musste und nach einem Werktag ersetzt werden konnte. Das betroffene Unternehmen erwirtschaftet mit 60 Mitarbeitern ca. acht Mio. Euro Umsatz pro Jahr. Die Durchlaufzeit der Aufträge beträgt sechs Wochen. Ca. 1400 Aufträge werden jährlich bearbeitet. Es ist ein ERP (Enterprise-Resource-Planning - Unternehmensressourcenplanung) und ein CAD System (Computer aided Design – rechnerunterstütztes Konstruieren) vorhanden.

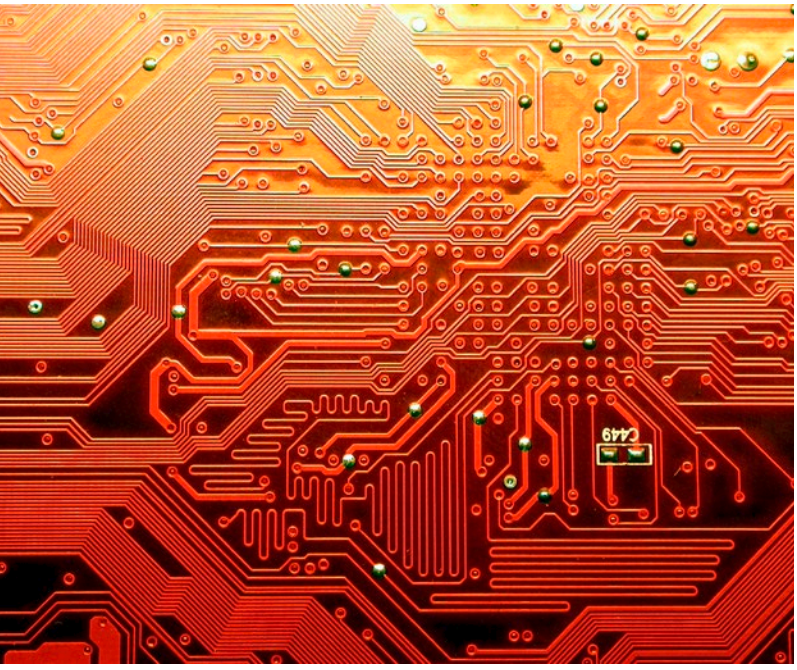


Bild: Klicker / pixelio.de

Folgen

Um die Kosten des Ausfalls zu beurteilen, wurde die gesamte Wertschöpfungskette des Kundenauftragsprozesses bewertet. Durch den Ausfall der EDV für einen Tag konnten drei Angebote über insgesamt 45.000 Euro nicht abgegeben werden. Es entstanden Leerzeiten und damit Überstunden in der Konstruktion und der Produktion für 40 Mitarbeiter. Das Unternehmen hatte einen Produktivitätsverlust von ca. 25.000 Euro pro Tag. Da das Unternehmen in einem Produktbereich als just in time Lieferant gelistet ist, erwarten die Kunden Realtime-Zugriff auf das Warenwirtschaftssystem. Der Ausfall führte daher automatisch zu einem EDV Audit (Risiko- und Schwachstellenanalyse) durch einen Kunden, mit einem entsprechenden Abweichungsbericht. Der Ausfall des Lieferscheindruckers stoppte für die Zeit die komplette Auslieferung mit der Folge, dass Standzeiten der LKW und Lieferterminverzögerungen zu Geld- und Imageverlust führten.

Lösung/Ergebnis

Der Kunde führte sofort ein Audit durch. Das Ergebnis war der Aufbau eines Risikomanagements und der Austausch von weiterer Hardware. Zusätzlich zeigten Datenschutzanalysen erheblichen Handlungsbedarf, um das Unternehmen, die Mitarbeiter, die Kunden und das Management abzusichern. Die unmittelbaren Schäden in Höhe von über 70.000 Euro konnten nicht abgewendet werden. Die schnelle Reaktion half, die nicht kalkulierbaren Folgekosten durch Verschiebung der Zeit- und Lieferpläne einzudämmen.

Expertentipp

Um Ausfallrisiken und Wartezeiten bei der Reparatur zu verhindern, sollten Hardware und Software möglichst innerhalb der vom Hersteller empfohlenen Zyklen aktualisiert werden. Dadurch steuert der Unternehmer den Ausfallzeitpunkt und kann notwendige Releasewechsel kontrolliert vorbereiten. Durch eine externe Potentialanalyse erhält das Thema die notwendige Transparenz und stärkt das Bewusstsein für diese und weitere Fragestellungen im Management eines Unternehmens.

Sicherheitsbereich:	**E-Mail – Virusbefall**
Unternehmen:	**B2B**
Unternehmensgröße:	**135 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**keine größeren Schäden durch schnelle Reaktion**

Tag des Vorfalls

Gegen 10:00 Uhr morgens wurde beim Abruf einer E-Mail, die vermeintlich von der Deutschen Post versendet wurde, ein Dateianhang geöffnet. Zehn Minuten später erschien ein Browserfenster. Das Schließen des Fensters oder ein Zugriff auf den Taskmanager waren nicht mehr möglich. Nach Reboot des Rechners blieb die Situation unverändert und der Kunde kontaktierte gegen 10:30 Uhr seinen IT-Dienstleister.

Kurzfristige/Langfristige Folgen

Durch die schnelle Reaktion des Anwenders konnten größere Schäden abgewendet werden. Der Schaden bestand so im Arbeitsausfall von etwa einem halben Tag und den Kosten des Servicetechnikers.

Lösung/Ergebnis

Durch eine Fern-Analyse wurde versucht, das Problem einzugrenzen. Die Anweisung wurde gegeben, den Rechner vom LAN zu trennen und herunterzufahren. Der Techniker war gegen 11:30 Uhr vor Ort und führte ein Reboot im abgesicherten Modus durch. Die Anmeldung erfolgte mit lokalem Administrator-Konto. Darauffolgend wurde das System überprüft und das Virus identifiziert. Kritische Einträge wurden gelöscht. Ein abschließender Reboot des Rechners fand um 13:00 Uhr statt: Anmeldung mit Nutzerkennung, Verbindung mit dem LAN, Download der aktuellen Signatur für das Anti-Malware-Programm und Scan aller Partitionen. Dieser Scan erbrachte keine weiteren Virenfunde.

Prävention

Eine Hauptursache des Virenbefalls bestand in der veralteten Version des eingesetzten Virenscanners, die es nicht erlaubte, das Virus bereits auf dem Mailserver zu erkennen. Daher sollte hier auf Aktualität geachtet werden.

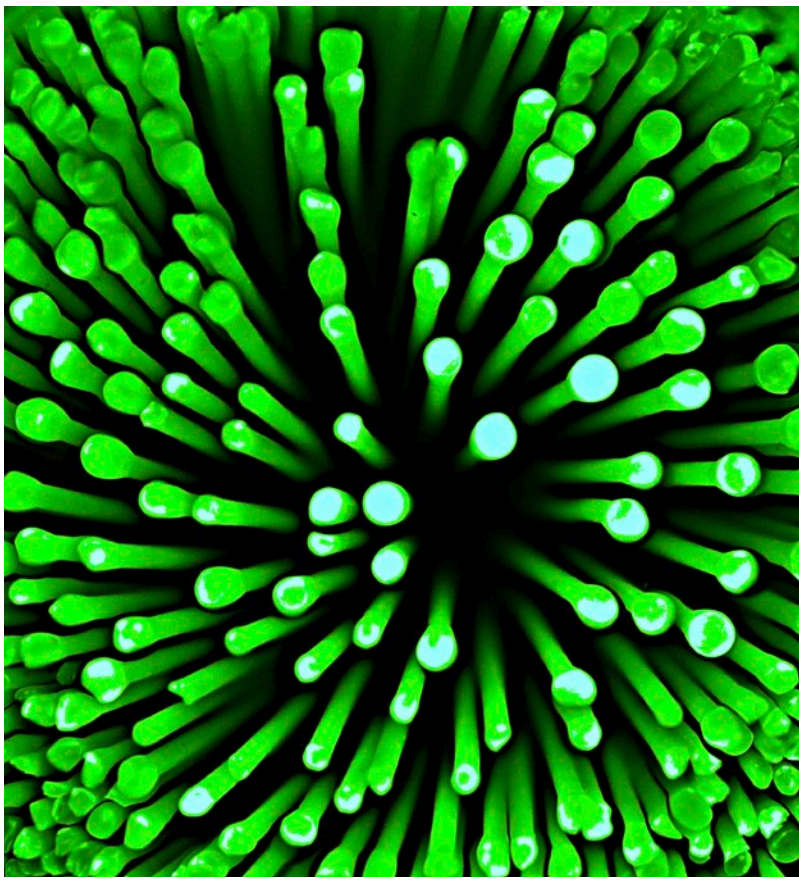


Bild: Gerd Altmann / pixelio.de

Expertentipp

Rechner, die im Verdacht stehen, von Viren befallen zu sein, sollten unmittelbar vom Netzwerk getrennt werden, damit eine Ausbreitung verhindert wird. Das unbedachte Öffnen von Email-Anhängen unbekannter Absender gilt es zu vermeiden. Vertrauliche E-Mails sollten prinzipiell verschlüsselt werden.

Sicherheitsbereiche:	**Mobile Endgeräte/Online Banking**
Unternehmensart:	**Dienstleistendes Unternehmen (B2B/B2C)**
Unternehmensgröße:	**Bis 10 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**ca. 25.000 Euro**

Der Tag des Vorfalls

Der Geschäftsführer eines mittelständischen Unternehmens befand sich auf einer Geschäftsreise und wollte die Wartezeit am Flughafen nutzen, um wichtige Banküberweisungen zu tätigen. Die notwendigen Unterlagen wie Rechnungsbelege, Zugangsdaten zum Onlinebanking, etc. hatte er mitgenommen. Auf seinem passwortgeschützten Laptop befanden sich PIN und TAN. Erfolgreich tätigte er seine Überweisungen und vergaß die Abflugzeit. Alles musste sehr schnell gehen. In letzter Minute erreichte er seinen Flug und bemerkte zu spät, dass sein ausgeschalteter Laptop samt Tasche zurückgeblieben war. Nach mehreren Stunden Flug hatte er Gelegenheit, bei seiner Bank anzurufen und den Verlust mitzuteilen.

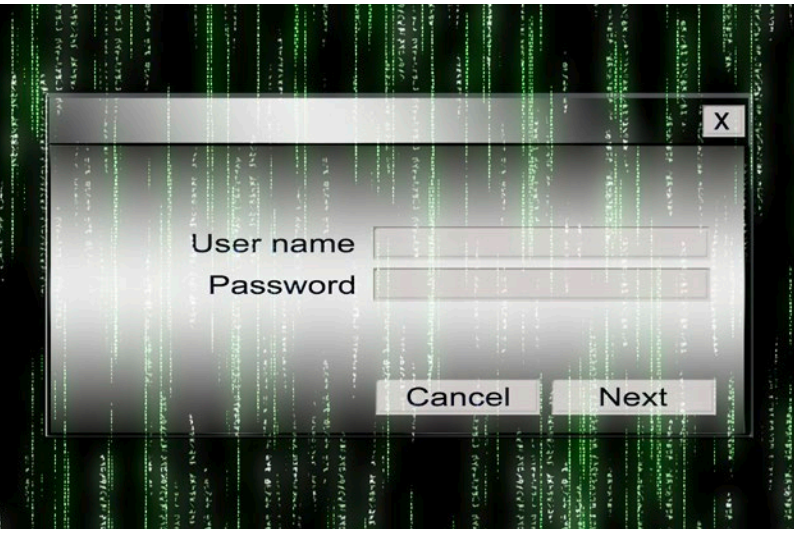


Bild: Gerd Altmann / pixelio.de

Folgen

Nach der Verlustmeldung informierte der Geschäftsführer seine Sekretärin. Sie prüfte die Konten und stellte das Fehlen von ca. 15.000 Euro (Höhe des Überweisungslimits) fest. Gravierender jedoch war der Verlust der Geschäftsdaten auf dem Laptop. Die letzten Bilanzdaten sowie die strategische Planung des Unternehmens waren auf dem Laptop gespeichert und gingen verloren. Sowohl operationelle als auch strategische Schäden sind nicht bekannt. Die unmittelbaren finanziellen Schäden beliefen sich auf 15.000 Euro. Die Neuanschaffung des Laptop und die Herstellung seiner Betriebsbereitschaft (ca. 1.000 Euro) sowie der unmittelbare Arbeitsaufwand verursachten weitere Kosten von ca. 10.000 Euro. Die zusätzlichen Arbeitsstunden wurden nicht dokumentiert.

Lösung/Ergebnis

Die Bankdaten wurden so schnell wie möglich gesperrt und eine Anzeige bei der Polizei aufgegeben, das Geld bleibt verschwunden.

Prävention

Durch Festplattenverschlüsselung und Richtlinien zum Umgang mit sensiblen Daten hätte der Schaden vermieden werden können. Passwortrichtlinien und eine genaue Kalkulation des Limits für Onlineüberweisungen sind unbedingt notwendig. Die Kosten für die Maßnahmen liegen weit unter dem Verlust der 15.000 Euro.

Expertentipp

Für die Absicherung von Diebstahl und/oder Beschädigung mobiler Endgeräte existieren Betriebsausfallversicherungen. Im vorliegenden Fall könnte es jedoch sein, dass das Unternehmen auf Grund von Fahrlässigkeit und organisatorischen Mängeln eine Mitschuld trägt und die Versicherung nicht gegriffen hätte. Schulungen und Sensibilisierungsmaßnahmen der Führungskräfte und Mitarbeiter sollten eingeführt werden. Angemessene Verhaltensregeln und der Umgang mit möglichen Gefährdungen sollten als integraler Bestandteil der Unternehmenskultur gelten.

Sicherheitsbereich:	**Server – Ausfall durch Wasserschaden**
Unternehmensart:	**Non Profit Unternehmen**
Unternehmensgröße:	**Bis 50 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**130.000 Euro**

Tag des Vorfalls

Der Serverraum des betroffenen Unternehmens befindet sich im Erdgeschoss eines fünfstöckigen Gebäudes. Über dem Serverraum befinden sich Räume mit wasserführenden Leitungen (WC + Küchen-Räume). Das Gebäude ist älterer Bauart und die Wasserleitungen sind bekanntermaßen sanierungsbedürftig. Ein Wasserrohrbruch in der 5. Etage oberhalb des Serverraumes führte dazu, dass sich das Wasser über vier Etagen seinen Weg bahnte, um dann umso heftiger das Erdgeschoss samt Serverraum zu fluten. Selbst das sofortige Abstellen des Wassers hatte keinen unmittelbaren Erfolg, da die vier Etagen zunächst „leer laufen" mussten und das Wasser über zwei Stunden in den Serverraum eindrang.

Folgen

Ein immenser Hardwareschaden, der Ausfall der gesamten IT für drei Tage waren die unmittelbaren Folgen. Die endgültige Beseitigung aller Schäden und Normalbetrieb war erst nach mehr als 14 Tagen möglich. Um den Schaden vollständig zu beheben, hatten alle Mitarbeiter über Wochen eine hohe Mehrbelastung. Das geschätzte Schadenvolumen beläuft sich auf ca. 130.000 Euro (inkl. der kalkulierten Personalmehrkosten).

Lösung/Ergebnis

Da alle Ethernetkabel des gesamten Unternehmens in einem Patchschrank im Serverraum zusammenliefen, war ein „Umzug" des Serverraumes nahezu unmöglich oder mit erheblichen Kosten verbunden. Der Datenschutzbeauftragte empfahl daher, Zwischendecke und Wände aus Plexiglas einzuziehen und alle Maschinen auf Podeste zu stellen.

Prävention

Eine Vermeidung des Schadens wäre vollständig möglich gewesen, da der Datenschutzbeauftragte das Problem im Vorfeld erkannt und die Geschäftsführung darüber in Kenntnis gesetzt hatte. Die oben erwähnte wasserdichte Schutzkonstruktion hätte Gesamtkosten von ca. 4.000 Euro zur Folge gehabt.

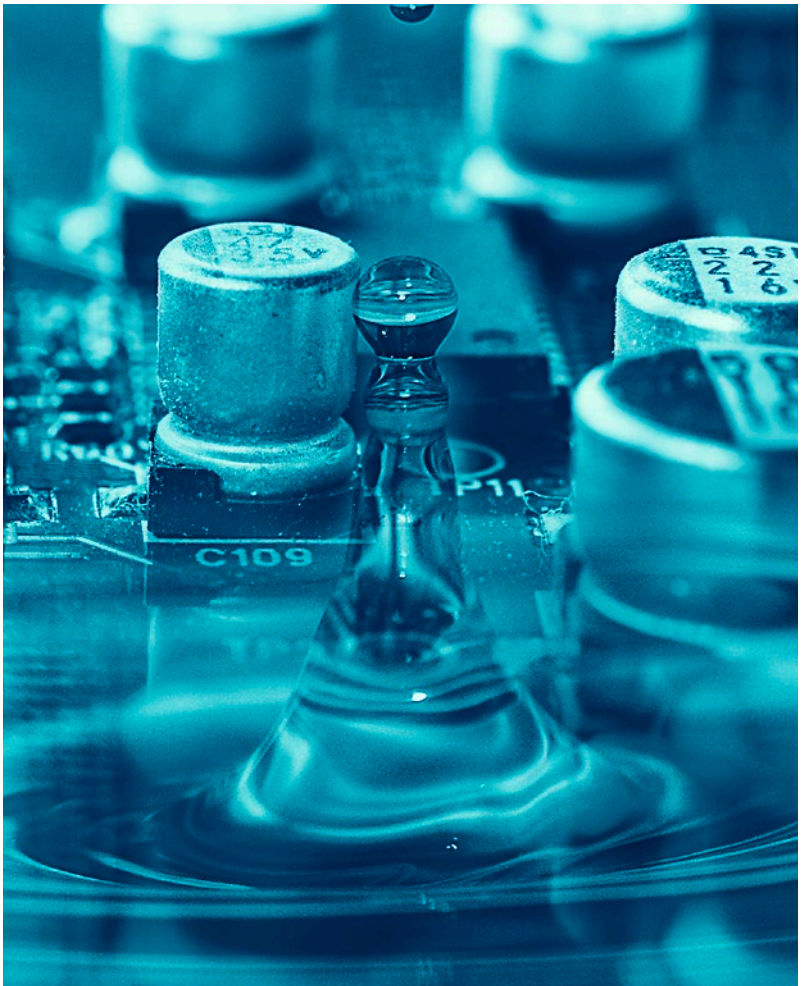


Bild: bildaspekt.de / pixelio.de

Expertentipp

Vorhandene und bekannte Risiken müssen ernst genommen werden. Jedes Unternehmen sollte sich einem Datenschutz-Check unterziehen. Hierbei wird ermittelt, wo ein Unternehmen den dringendsten Handlungsbedarf hat, und zwar nicht nur im Rahmen gesetzlicher Verpflichtungen und zum Schutz für die personenbezogenen Daten, sondern zur Sicherheit aller Unternehmensdaten und damit zum Schutz des gesamten Unternehmens.

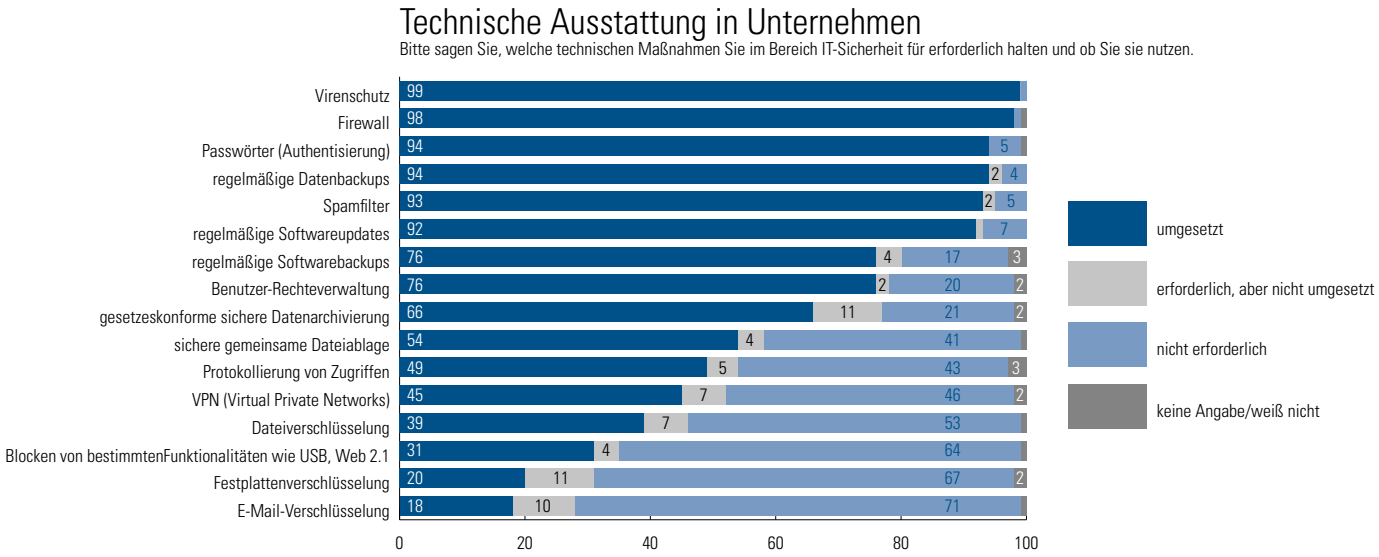
Sicherheitsbereich:	**Back Up – Datensicherung**
Unternehmensart:	**Produzierendes Unternehmen als Zulieferer B2B**
Unternehmensgröße:	**bis 50 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**60.000 Euro**

Der Tag des Vorfalls

Beim Upgrade der branchenspezifischen Software wurde durch einen Administrationsfehler die SQL-Datenbank (SQL = Datenbanksprache) bei der Datenreorganisation zerstört. Die kundenspezifischen Daten (Stammdaten, Bestelldaten, Auftragsstatus, Lieferungs- und Rechnungsdaten) konnte das System nicht mehr den richtigen Kundennummern zuordnen. Die alte Konfiguration musste wieder hergestellt werden. Das Sicherungsband vom letzten Arbeitstag wurde eingelegt. Nun sollte die Backup-Software gestartet und der Rücksicherungsvorgang aktiviert werden. Dabei stellte sich heraus, dass die Backup-Software gar nicht installiert war. Die Datensicherung war seit der Inbetriebnahme der neuen Hardware (vor ca. neun Monaten) nicht gelaufen. Das Bandlaufwerk hat zwar den Wechsel der Datensicherungsbänder quittiert, jedoch wurde durch mangelnde Kontrolle des Kunden und Unkenntnis des Administrators die Datensicherungssoftware gar nicht installiert und keine Datensicherungsroutinen eingestellt.

Folgen

Es entstand ein Produktionsausfall von insgesamt drei Tagen und damit ein Umsatzausfall von ca. 45.000 Euro. In dieser Zeit konnten im betroffenen Unternehmen keine auftragsbezogenen Daten verarbeitet werden. Dazu kommt ein Aufwand von min. 15.000 Euro für die Wiederherstellung der Daten sowie die Aufarbeitung der drei verlorenen Tage.



Quelle: WIK-Consult Studie Sicherheitsniveau in KMU 2011/12

Lösung/Ergebnis

Die einzige Möglichkeit den Datenbestand wiederherzustellen war, die Daten durch den Softwarehersteller wieder zu reorganisieren. Dazu musste der Datenbestand per externen Datenträger an den Softwarehersteller gegeben werden. Dieser benötigte dann zwei Tage zur Wiederherstellung der Daten.

Prävention

Allein durch die Prüfung einer Rücksicherung der Datensicherung durch die IT-Abteilung hätte dieser Schaden vermieden werden können. Der Zeitaufwand hierfür beträgt ca. eine Stunde und wäre im Rahmen der normalen Tätigkeiten zu erledigen gewesen.

Expertentipp

Es ist hilfreich, zumindest einmal einen kompletten Ernstfall durchzuspielen und dabei die Daten komplett von den Backup-Medien zu lesen. Die meisten Fehler zeigen sich recht schnell bei einem Wiederherstellungstest.

Sicherheitsbereich:	**E-Mail – Vertretungsregelung**
Unternehmen:	**Produzierendes Unternehmen B2B**
Unternehmensgröße:	**Bis 100 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**über 10.000 Euro**

Tag des Vorfalls

In einem mittelständischen Unternehmen ist die aktuelle Fassung der CAD-Zeichnungen von Kundenprodukten nicht aufzufinden. Schließlich wird diese in der Mailbox eines Mitarbeiters vermutet, der sich im Urlaub befindet. Da die Zeichnungen im Hause des Lieferanten modifiziert wurden, kann auch der Kunde nicht aushelfen. Eine fehlende Richtlinie zum Umgang mit E-Mail sowie eine nicht vorhandene Archivierung verzögern das Auffinden der betreffenden Zeichnung und somit den umgehenden Beginn der Teileproduktion sowie die rechtzeitige Fertigstellung des Auftrages. Der im Ausland befindliche Mitarbeiter konnte schließlich nach einigen Tagen erreicht werden, sodass die Herausgabe der Anmeldedaten durch ein festgelegtes Rückrufverfahren möglich wurde.

Bild: Andreas Hermsdorf / pixelio.de

Folgen

Die Verzögerung in der Produktion führte zum Verlust des Kunden, Schadenersatzzahlungen wegen nicht rechtzeitiger Auslieferung und einer Beschädigung der Reputation des Unternehmens wegen Nichtergreifung von Maßnahmen zur Absicherung des Risikos. Der unmittelbare Schaden lag über 10.000 Euro, Folgeschäden durch anderenfalls erteilte weitere Aufträge lassen sich nur schlecht beziffern.

Lösung/Ergebnis

Als Konsequenz auf den Vorfall wurden Richtlinien für den Gebrauch der IT, speziell E-Mail, entwickelt und eingeführt. Durch Vertretungsregelungen wird der wechselseitige Zugriff auf produktionskritische Informationen auch bei Ausfall von Mitarbeitern gewährleistet. Zusätzlich hat das Unternehmen technische Vorkehrungen zum Schutz vor Verlust von Informationen getroffen. Ein vorgeschalteter Viren- und Spamfilter hält Schadcode aus dem Unternehmen fern. Mit einer Appliance zur Archivierung aller im Unternehmen empfangenen und versandten E-Mails ist der Zugriff durch Befugte auch auf versehentlich wie absichtlich gelöschte E-Mails unter geregelten Voraussetzungen möglich. Da das Unternehmen mit teils hochinnovativen Kunden zusammenarbeitet, wird zur Gewährleistung eines vertraulichen E-Mailkontaktes eine Verschlüsselungslösung zusätzlich eingeführt.

Prävention

Durch den Verlust von Auftrag und Kunde ist dem Unternehmen Umsatz in fünfstelliger Größenordnung direkt verloren gegangen. Eine Analyse ergab, dass es bereits in der Vergangenheit Zeitverluste und Produktivitätsverluste durch fehlende Informationen in E-Mails gab. Die Erkenntnis, dass E-Mail in der Praxis eines produzierenden Unternehmens kritisch sein kann, wurde erst durch den Schadensfall gewonnen. Eine frühzeitigere Investition in organisatorische wie technische Maßnahmen hätte Umsatz- und Kundenverlust vermeiden können.

Expertentipp

Die Kommunikation via E-Mail bzw. der laxe Umgang mit diesbezüglichen Sicherheitsfragen sorgt zunehmend für Risiken in Unternehmen. Mit der selbstverständlichen Nutzung von E-Mail sollte auch die Absicherung dieses wichtigen Kommunikationsmediums einhergehen. Die Einführung hochwertiger Filtermechanismen hält Viren und Trojaner vom Unternehmen fern und steigert die Produktivität. Nachrichtenarchivierer ermöglichen einen gesicherten Zugriff auf versandte und erhaltene E-Mails und erfüllen, wenn richtig implementiert, noch nebenher gesetzliche Vorschriften. Nachrichten, die Sie üblicherweise keiner Postkarte anvertrauen würden, gehören zudem verschlüsselt.

Sicherheitsbereich:	**Mobile Endgeräte – Diebstahl**
Unternehmensart:	**Produzierendes Unternehmen (B2C)**
Unternehmensgröße:	**Bis 500 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**5.000 Euro**

Bild: tommyS / pixelio.de

Tag des Vorfalls

Zur Vertragsverhandlung nimmt der Vertriebsleiter eines mittelständischen Unternehmens das Angebot und alle damit im Zusammenhang stehenden Unterlagen (Lieferanten-Daten, Leistungsbeschreibung, Kalkulation etc.) auf seinem Notebook mit. Beim Aufenthalt auf dem Flughafen Frankfurt/Main wird die Reisetasche mit Notebook gestohlen. Das Notebook ist nur durch ein einfaches Passwort geschützt. Das Passwort wird geknackt und alle Informationen liegen in Klartext vor. Der Vertriebsleiter bekommt wenig später einen anonymen Anruf, dass er sein Notebook gegen Zahlung von 10.000 Euro in bar zurück bekommt. Zur Bestätigung wurden Beispiele aus der Kalkulation genannt.

Folgen

Obwohl der Diebstahl sofort bemerkt wurde, konnte der Täter nicht gestellt werden.

Die Vertragsverhandlung musste kurzfristig abgesagt werden. Der Kunde war über die Absage und Preisgabe von Informationen verärgert. Der Auftrag ging an einen Mitbewerber. Die Kosten für die Vorbereitung des Angebotes und zur geplanten Vertragsverhandlung beliefen sich auf ca. 5.000 Euro. Der Gewinnausfall konnte nicht beziffert werden. Das Vertrauen des Kunden in das Unternehmen ist durch diesen Vorfall geschwächt worden. Da sich das Unternehmen gegen den Rückkauf des Notebooks entschieden hatte, musste ein neues Notebook beschafft werden. Ein Imageverlust oder andere Folgen konnten nicht festgestellt werden.

Lösung/Ergebnis

Für diesen Fall gab es keine Lösung.

Prävention

Zur Vermeidung solcher Ereignisse sind verschiedene Szenarien möglich:

- Verschlüsselung der Dateien auf dem Notebook
- Einrichtung einer Authentifizierung vor dem Start
- Transport der Daten außerhalb des Notebooks (verschlüsselter USB-Stick)
- Bereitstellung der Daten im Web über geschützte Verbindungen

Das Unternehmen führte nach diesem Vorfall eine zentrale Verschlüsselungslösung ein und stattete die Nutzer mobiler Geräte mit einem USB-Stick zur Verschlüsselung aus. Dafür war eine Investition von ca. 5.000 Euro notwendig.

Expertentipp

Der Verlust mobiler Geräte ist kein Einzelfall: Jede Woche werden 300 Laptops auf dem Frankfurter Flughafen gefunden. Bereits mit geringen Investitionen können die Risiken für einen Datenverlust oder Datenmissbrauch stark minimiert werden. Der immaterielle Schaden bei solchen Vorfällen ist oft höher als der materielle Schaden.

Sicherheitsbereich:	**Geschäftsgeheimnisse – Sicherheitsrichtlinie**
Unternehmensart:	**Dienstleistendes Unternehmen (B2C)**
Unternehmensgröße:	**Bis 500 Mitarbeiter**
Unmittelbarer finanzieller Schaden:	**nicht zu beziffern**

Der Tag des Vorfalls

Mit dem Ausscheiden eines leitenden Mitarbeiters verließen auch streng vertrauliche Informationen wie Kundendaten, Marketing- und Expansionspläne ein mittelständisches Unternehmen. Es wurde Anzeige erstattet, der Rechtsstreit endete in einem Vergleich.

Folgen

Der ehemalige Mitarbeiter wurde schnell zum Wettbewerber und eröffnete ein Konkurrenzgeschäft. Hierfür benutzte er die entwendeten Informationen und warb einen Teil der Kunden ab. Im geschädigten Unternehmen wurde eine Neuregelung der IT-Zugriffe und betriebsinternen Abläufe notwendig. Zudem war das Betriebsklima durch Misstrauen langfristig geschädigt, Marketingstrategien und Expansionspläne waren nicht mehr umsetzbar und finanzielle Schäden durch hohe Anwalts- und Gerichtskosten sowie Umsatzeinbußen durch Kundenabwerbung mussten kompensiert werden. Neben einem hohen finanziellen Schaden hatte das Unternehmen auch einen Imageverlust bei seinen verbliebenen Kunden zu verkraften.

Bild: Rainer Sturm / pixelio.de

Lösung/Ergebnis

Neue Strukturen und eine Lösung für die Gefahrenabwehr mussten eingeführt werden. Das Problem wurde durch Sensibilisierung der Mitarbeiter und Einführung einer Information Rights Management Anwendung gelöst. Diese ermöglicht die vollständige Kontrolle über die Nutzung und den Zugriff auf sensible Firmendaten. Datenklau und unberechtigte Datennutzung werden hierdurch unterbunden. Der Schaden konnte nicht mehr eingedämmt werden, wird aber durch die ergriffenen Maßnahmen in Zukunft nicht mehr auftreten.

Prävention

Durch geeignetes Risikomanagement, Bewusstseinsschaffung für vertrauliche Informationen und Einsatz geeigneter Maßnahmen wie IRM hätte der Schaden vermieden werden können. Eine Investition in diese Maßnahmen und in moderne Sicherheitslösungen liegt nur bei einem Bruchteil der Schadensummen.

Expertentipp

Tipps zur Minimierung des Datenverlustes von Betriebsgeheimnissen:

- Daten klassifizieren: Welche Daten im Unternehmen sind schützenswert?
- Zugriffe identifizieren: Mit welchen Geräten wird auf welche Daten zugegriffen?
- Speicherorte festlegen: Wo werden Daten abgelegt?
- Zugang limitieren: Wer muss wie, wann und wo auf sensible Daten zugreifen können?
- Schutzmaßnahmen installieren: Sicherheitsrichtlinien mit Überwachung einführen und geeignete Tools dafür auswählen

Sicherheitsbereich:	**E-Mail – Verschlüsselung**
Unternehmensart:	**Produzierendes Unternehmen als Zulieferer (B2B)**
Unternehmensgröße:	**Bis 100 Mitarbeiter**
Unmittelbare finanzielle Schäden:	**10.000 Euro**

Tag des Vorfalls
Für ein neues Projekt schickte ein Unternehmen ein Angebot mit vielen Details über den Kunden an eine falsche Mailadresse. Der falsche Empfänger bemerkte den Fehler und leitete die Mail an den richtigen Empfänger weiter.

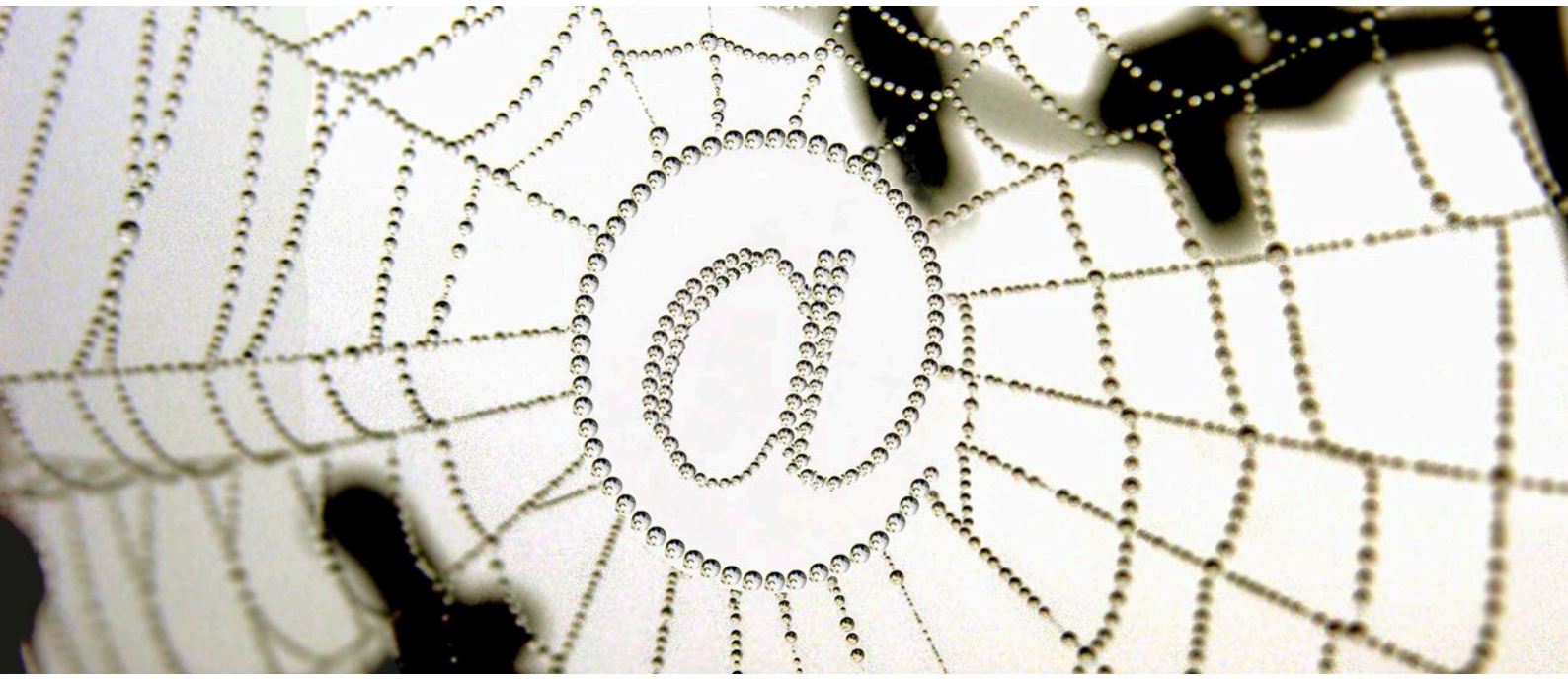
Folgen
Der Auftraggeber war verärgert und beschwerte sich über die Preisgabe von Informationen an Dritte und forderte einen Schadenersatz von 10.000 Euro. Der Auftraggeber machte von seinem außerordentlichen Kündigungsrecht Gebrauch. Das Unternehmen musste den Schadenersatz in Höhe von 10.000 Euro begleichen. Der Gewinnausfall und der Imageverlust konnten nicht beziffert werden. Für das Projekt müssen neue Abnehmer akquiriert werden.

Lösung/Ergebnis
Für diesen Fall gab es keine Lösung.

Prävention durch Investition
Durch eine Verschlüsselung der E-Mail wäre sie für den falschen Empfänger nicht lesbar gewesen. Das Unternehmen führte nach diesem Vorfall eine zentrale Verschlüsselungslösung ein und stattete die externen Nutzer und die Kommunikationspartner mit einem USB-Stick zur Verschlüsselung aus. Dafür war eine Investition von ca. 5.000 Euro notwendig.

Expertentipp
Der Austausch von Daten per E-Mail ist zu einem etablierten Verfahren geworden. Durch Fehler oder gezieltes „Abhören" des Mail-Verkehrs können Daten in falsche Hände geraten und missbraucht werden. Beim Austausch von personenbezogenen und Geschäftsdaten sollte dieses Risiko besonders berücksichtigt werden. Der Einsatz einer Verschlüsselungslösung verhindert das Lesen von Daten durch Dritte.

Bild: pepsprog / pixelio.de



Sicherheitsbereich:	**IT gesteuerte Produktion – Internetportal**
Unternehmensart:	**Dienstleistendes Unternehmen (B2C)**
Unternehmensgröße:	**Bis 500 Mitarbeiter**
unmittelbare finanzielle Schäden:	**ca. 500.000 Euro**

Der Tag des Vorfalls

Der Kunde betreibt im Internet eine Plattform, über die der gesamte Umsatz generiert wird. Auf der Plattform kann man u.a. Nachrichten an das Unternehmen schicken (Feedback-Page). Diese Feedback-Page ermöglichte es zudem, dass der Endkunde Anhänge mitschicken kann. Für die Anhänge gab es keine Größenbeschränkung und auch das Absenden der Nachricht wurde nicht abgesichert. Hacker aus dem Ausland hatten dies erkannt, das System mit automatisch erzeugten Nachrichten mit relativ großen Anhängen geflutet und damit lahmgelegt.

Folgen

Der Angriff wurde erst bemerkt, nachdem das Gesamtsystem zum Stillstand kam. Es war mit der Abarbeitung der Nachrichten und der Anhänge so ausgelastet, dass es für neue Endkunden nicht mehr möglich war, sich anzumelden und Geschäft zu generieren. Die Nachrichten konnten nicht einfach vollständig gelöscht werden, da sich im selben Ordner auch Nachrichten von Kunden und Systemnachrichten befanden. Die relevanten Nachrichten wurden gesichert und die „bösen" Nachrichten mussten manuell entfernt werden. Der Rest wurde dann wieder in die Nachrichten-Queue zurück geschoben, damit das System diese Nachrichten abarbeiten konnte.

Da die Geschäfte zeitkritisch sind und zu keinem späteren Zeitpunkt nachgeholt werden konnten, ist dem Unternehmen ein wirtschaftlicher Schaden in Höhe von ca. 500.000 Euro entstanden. Die hohe Summe kam dadurch zustande, dass zeitgleich eine sehr große Werbeaktion zur Neukundengewinnung lief, diese aber erfolglos blieb; Neukunden konnten nicht generiert werden – vorhergegangene Werbeaktionen brachten großen Zuwachs. Zudem konnten Bestandskunden keine neuen Aufträge platzieren. Da die erforderlichen Änderungen im normalen Softwareentwicklungsprozess mit gemacht wurden, entstanden darüber hinaus keine Kosten; der langfristige Schaden ist schwer zu beziffern.

Bild: Gerd Altmann / pixelio.de

Lösung/Ergebnis

Die Lösung war sehr einfach: Einbau einer CAPTCHA-Funktion auf der Feedbackseite und eine Größenlimitierung für mitgesendete Anhänge auf 1 Mbyte.

Prävention

Durch einen professionell durchgeführten Test für Online-Plattformen hätte der Unfall vermieden werden können.

Expertentipp

Wenn der Kunde seine Software selber entwickelt, sind solche Fehler nicht zu vermeiden. Die Mitarbeiter, zum Beispiel Designer, Entwickler usw., übersehen relativ schnell diese Art offensichtlicher Risiken. Der Fokus bei der Anwendung wurde und wird auf das Geschäftsziel gerichtet. Wichtig wäre es aber gewesen, auch technische Belange, Sicherheit des Systems, Ausfallszenarien o.ä zu betrachten.

[m]IT Sicherheit Tipps

Sicherheitsbereich: Redundante Systeme
Expertentipp:

- Schalten Sie mehrerer Internetzugänge zusammen. So erhalten Sie eine Redundanz, so dass einzelne Anschlüsse ausfallen können, ohne dass der Betrieb gestört wird.
- Schalten Sie zwei oder mehrere Firewalls zu einem Cluster zusammen, so dass der Ausfall eines Gerätes nicht zum Ausfall der Internetanbindung führt.
- Entscheiden Sie sich am besten für mindestens einen Business-Tarif. Somit haben Sie die Möglichkeit, feste IP-Adressen zu nutzen, erhalten vertraglich garantierte Entstörzeiten und der Anbieter ist bei längeren Ausfallzeiten haftbar für den entstandenen Schaden.

Sicherheitsbereich: Back Up
Expertentipp:

- Spielen Sie in Ihrem Unternehmen einen Ernstfall durch und prüfen Sie die Daten von den Backup-Medien, um bei dem Wiederherstellungstest die Fehler direkt zu erkennen.

Sicherheitsbereich: Server
Expertentipp:

- Aktualisieren Sie Hardware und Software innerhalb der vom Hersteller empfohlenen Zyklen. Sie verhindern so Ausfallrisiken und Wartezeiten bei der Reparatur.

Sicherheitsbereich: Geschäftsgeheimnisse
Expertentipp:

- Klassifizieren Sie die Daten, die schützenswert sind.
- Identifizieren Sie, mit welchen Geräten auf welche Daten zugegriffen wird.
- Legen Sie die Speicherorte Ihrer Daten fest.
- Limitieren Sie den Zugang auf sensible Daten.
- Führen Sie Sicherheitsrichtlinien ein und stellen Sie sicher, dass diese eingehalten werden.

Bild: Gerd Altmann / pixelio.de

Sicherheitsbereich: E-Mail
Expertentipp:

- Verschlüsseln Sie prinzipiell vertrauliche E-Mails. Nachrichten, die Sie einer Postkarte nicht anvertrauen würden, sollten nicht unverschlüsselt versandt werden.
- Vermeiden Sie das unbedachte Öffnen von Email-Anhängen unbekannter Absender.
- Trennen Sie infizierte Rechner unmittelbar vom Netzwerk, wenn ein Virus über E-Mail in Ihr System gelangt ist, damit eine Ausbreitung verhindert wird.
- Führen Sie hochwertige Filtermechanismen ein, um Viren und Trojaner vom Unternehmen fern zu halten und die Produktivität zu steigern.
- Nutzen Sie Nachrichtenarchivierer, um einen gesicherten Zugriff auf versandte und erhaltene Emails zu ermöglichen. Richtig implementiert, erfüllen Sie damit gleichzeitig gesetzliche Vorschriften.

Sicherheitsbereich: Mobile Endgeräte
Expertentipp:

- Verschlüssen Sie Daten auf mobilen Datenträgern und Endgeräten.
- Nutzen Sie Betriebsausfallversicherungen für die Absicherung von Diebstahl und/oder Beschädigung mobiler Endgeräte.
- Führen Sie angemessene Verhaltensregeln und Sensibilisierungsmaßnahmen für den Umgang mit möglichen Gefährdungen als integralen Bestandteil der Unternehmenskultur ein.

Sicherheitsbereich: Telefonie
Expertentipp:

- Achten Sie auf Vertraulichkeit: unverschlüsselte Gespräche – insbesondere bei IP-Telefonie – können mitgehört werden.
- Misstrauen Sie unbekannten Telefonnummern: diese können gefälscht werden.

Sicherheitsbereich: Mitarbeiter
Expertentipp:

- Investieren Sie in eine Sicherheitsrichtlinie und Datenschutzvereinbarung für Mitarbeiter sowie in die entsprechende Software zur Überprüfung der Einhaltung.

Dank

Der BVMW bedankt sich bei der Task-Force „IT-Sicherheit in der Wirtschaft“
des Bundesministeriums für Wirtschaft und Technologie für die Förderung dieses Projekts.

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Diese Broschüre wurde in Zusammenarbeit mit den folgenden Mitgliedern unsere Best-Practice KMU Expertengruppe erstellt. Die verwendeten Beispiele sind anonymisiert und wurden von den Teilnehmern der Expertengruppe zusammengestellt. Diese waren im Rahmen ihrer Tätigkeiten für die Eindämmung und Behebung der Schäden zuständig.

Commehr GmbH
www.commehr.de
info@commehr.de
Tel. +49 30 890070
Friedrich-Karl-Straße 18
12103 Berlin

COMPASS Berater für Datenverarbeitung und Training GmbH
www.compass.de
service@compass.de
Tel. +49 2235 9541-0
Dieselstraße 14
50374 Erftstadt

EMC Köln GmbH
www.emc-koeln.com
info@emc-koeln.com
Tel. +49 2222 9631-65
Kleinstraße 14
53332 Bornheim – Hersel

Giegerich & Partner GmbH
www.giepa.de
info@giepa.de
Tel. +49 6103 588131
Robert-Bosch-Straße 18
63303 Dreieich

Ibykus AG
www.ibykus.de
info@ibykus.de
Tel. +49 361 44100
Herman-Hollerith-Straße 1
99099 Erfurt

LT Memory GmbH
www.ltmemory.de
info@ltmemory.de
Tel. +49 30 7109000
Giesensdorfer Straße 29
12207 Berlin

mb-datenschutz
www.mb-datenschutz.de
info@mb-datenschutz.de
Tel. +49 30 36727755-0
Jänickendorfer Weg 17
13591 Berlin

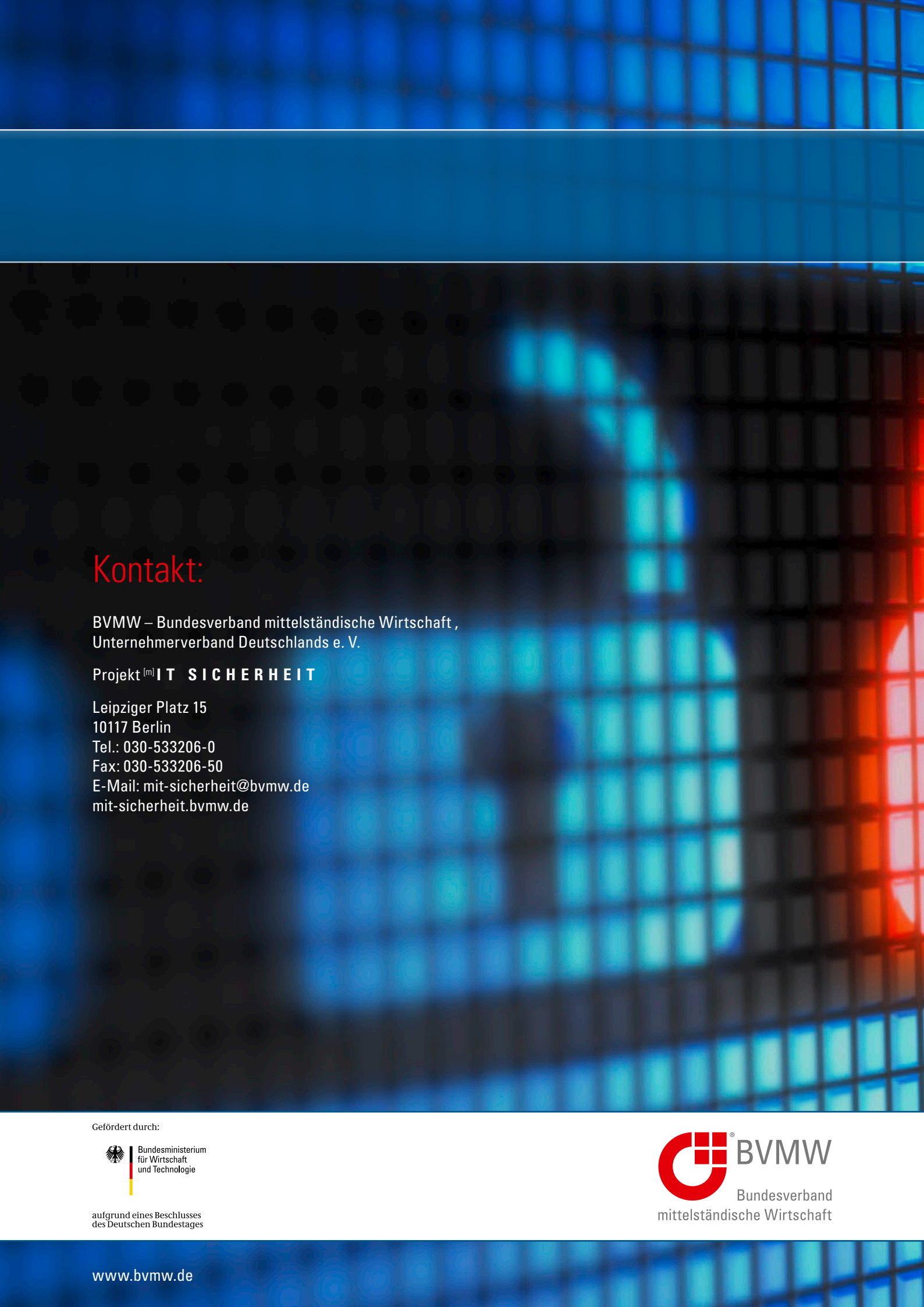
Pohl Consulting Team GmbH
www.pct.eu
info@pct.eu
Tel. +49 5691 8900501
Mengeringhäuser Straße 15
34454 Bad Arolsen

procilon IT-Solutions GmbH
www.procilon.com
info@procilon.de
Tel. +49 34298 4878-10
Leipziger Straße 110
04425 Taucha bei Leipzig

Pro-Icon
www.pro-icon.de
info@pro-icon.de
Tel. +49 2302 933029
Akazienweg 7
58452 Witten

Secianus Karner & Schröppel, Partnerschaft
www.secianus.de
info@secianus.de
Tel. +49 175 2239010
Hanserauweg 3
92342 Freystadt

Franz J. Steppe Interim Management
www.franzsteppe.com
post@franzsteppe.com
Tel. +49 89 45221870
Tizianstraße 119
80 638 München



Kontakt:

BVMW – Bundesverband mittelständische Wirtschaft ,
Unternehmerverband Deutschlands e. V.

Projekt [m] IT SICHERHEIT

Leipziger Platz 15
10117 Berlin
Tel.: 030-533206-0
Fax: 030-533206-50
E-Mail: mit-sicherheit@bvmw.de
mit-sicherheit.bvmw.de

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

BVMW
Bundesverband
mittelständische Wirtschaft