IT-Sicherheit: „Wesentlich mehr Einfallstore als vor der Pandemie“

Viele Unternehmen haben zu Beginn der Pandemie die Erreichbarkeit priorisiert und dabei die Sicherheit vernachlässigt. Prof. Kai-Oliver Detken, Geschäftsführer des Softwarehauses und Systemintegrators Decoit GmbH, erklärt im Interview die wichtigsten aktuellen Herausforderungen für Geschäftsführungen.

Interview: Axel Kölling, Foto: Jörg Sarbach

Sie haben kürzlich zusammen mit Prof. Dr. Evren Eren von der Hochschule Bremen das „Handbuch Datensicherheit“ veröffentlicht. Warum war es Zeit für einen neuen Ratgeber in diesem Bereich?

Mein Co-Autor Evren Eren und ich wurden von einem Verlag angesprochen, der sich vor allem an Kommunen richtet. Verwaltungen sind mit dem Thema IT-Sicherheit zunehmend überfordert. Kleinen und mittleren Unternehmen geht es sehr ähnlich, darum richten wir uns mit dem Buch auch an sie.

Prof. Kai-Oliver Detken, Geschäftsführer des Softwarehauses und Systemintegrators Decoit GmbH.

Die Kommunen und Betriebe haben oft keine IT-Sicherheitsexperten im eigenen Hause und keinen genauen Überblick über die gesetzlichen Vorschriften. Sie benötigen Orientierung, wenn sie mit Schlagworten wie Digitalisierung, Meldegesetz oder IT-Sicherheitsgesetz konfrontiert werden. Wir versuchten, da Struktur hineinzubringen: Was sind die dringendsten Themen? Was steht hinter den Schlagworten? Wie geht man damit um, nicht nur aus technischer Sicht, sondern auch unter rechtlichen Aspekten?

Spüren Sie mit Ihrem Unternehmen eine große Nachfrage nach Sicherheitslösungen?

Sicherheit ist für uns ein großer Schwerpunkt im Softwarebereich, aber das Thema kommt meistens im Rahmen von Infrastruktur-Projekten auf. Viele kleine und mittelständische Unternehmen tun sich mit IT-Sicherheit immer noch schwer, weil es erstmal keine Prozessoptimierung ist. Sie bemerken nur die Kosten, aber keine Vorteile. Deswegen investieren sie lieber in Dinge, die sie prozesstechnisch weiterbringen, zum Beispiel Warenwirtschaftssysteme.

Sehen Sie Unternehmen, die mit dieser Herangehensweise Probleme bekommen?

Ja, auf jeden Fall. Gerade die Verschlüsselungstrojaner, die es in letzter Zeit gegeben hat, haben auch einige unserer Kunden getroffen. Die Kriminellen verschlüsseln dabei das IT-System und verlangen Lösegeld, um es wieder freizuschalten. Unter den Betroffenen waren von kleinen bis zu richtig großen Unternehmen alle dabei. Dort wurden einige Dinge nicht beherzigt, die wir in der Konzeption empfohlen hatten, sodass dann nicht nur der Hauptserver verschlüsselt war, sondern auch das Backup-System. Oft führt erst das „Lernen durch Schmerzen“ zu Änderungen.

Haben sich die Bedrohungen seit Beginn der Pandemie verändert?

Ja – dadurch, dass wir jetzt verteilt arbeiten. Als es im letzten Jahr losging, sind viele spontan ins Home

Die wichtigsten Empfehlungen im Überblick:

- Grundsätzlich nicht nur die Verfügbarkeit des Systems priorisieren, sondern auch die Sicherheit
- Durchgehend Verschlüsselung nutzen, auch bei den Emails
- Alle Systeme im Unternehmen auf dem neuesten Stand halten – besonders die, die von außen zugänglich sind
- Ein einfacher Virenschutz und eine einfache Firewall reichen nicht mehr aus, weil die Bedrohung komplexer geworden ist
- Keine Email-Links anklicken – immer ins Kundenportal gehen und dort anmelden
- Sichere Passwörter verwenden und in einem Passwortmanager speichern

> *Sicherheit ist in vielen IT-Projekten noch kein integraler Bestandteil – das ist einer der Hauptfehler.*
>
> *Prof. Kai-Oliver Detken*

Office ausgewichen. Da wurde erstmal hauptsächlich darauf geachtet, dass die Leute im Home Office arbeiten können, aber die Sicherheit wurde nicht unbedingt in Frage gestellt. Viele haben beispielsweise ihren privaten Rechner genommen – in einer privaten Umgebung, die schlechter gesichert ist als ein Unternehmen. Dementsprechend hat man jetzt im Unternehmen wesentlich mehr Einfallstore als vor der Pandemie.

Gibt es bestimmte Fehler, die immer wieder gemacht werden?

Dem Druck des Tagesgeschäfts geschuldet, wird in vielen Unternehmen oft zwar darauf geachtet, dass die Systeme 24/7 zur Verfügung stehen, aber nicht darauf, ob sie vernünftig abgesichert sind. Da wird IT-Sicherheit sogar manchmal als Problem gesehen, weil Sicherheitssysteme die Verfügbarkeit beeinträchtigen können, wenn sie Sicherheitslücken bemerken.

Häufig wird IT-Sicherheit nicht als integraler Bestandteil der Netzwerk-Infrastruktur gesehen, sondern nur als Anhängsel. Zuerst wird geguckt: „Welche Rechenleistung brauchen wir, wie schnell muss das System sein, wieviel Speicher muss vorhanden sein, können wir das hochverfügbar machen?“ Die IT-Sicherheit kommt erst im Nachhinein – und meistens erst, wenn etwas passiert ist. Dann wird beispielsweise darüber nachgedacht, USB-Ports abzusichern, weil ein Mitarbeiter mit den Kundendaten auf einer USB-Festplatte spazieren gegangen ist und das Unternehmen verlassen hat.

Was sind im Moment die häufigsten Empfehlungen, die Sie aussprechen?

Es gibt eine ganze Menge zu beachten. Man sollte nicht unbedingt mit seinem privaten System arbeiten. Auch aus Datenschutzgründen ist es schwierig, wenn private und geschäftliche Daten vermischt werden. Man sollte dann entweder die Geschäftsdaten nur mit einer verschlüsselten Festplatte nutzen oder ein ganz eigenes Gerät bekommen. Das ist ein Grund, warum Laptops im letzten Jahr so gut wie ausverkauft waren. Die Firmengeräte sollten natürlich genauso sicher eingerichtet sein wie die Geräte in der Firma selbst. Für den Kontakt mit dem Firmennetzwerk sollten nur gesicherte Verbindungen genutzt werden. In vielen Projekten haben wir auch Terminal-Server benutzt, bei denen man einfach nur ein Abbild seines eigenen Desktops im Home Office bekommt – wenn der Rechner infiziert wird, bleibt der virtuelle Desktop davon unberührt.

Ansonsten ist es auch wichtig, dass man die Antiviren-Software, also den Schutz der Rechner, zentral administriert. So weiß man, dass sie auf dem aktuellen Stand und eingeschaltet ist. Das ist aber in vielen Unternehmen nicht der Fall.

Empfehlenswert ist es außerdem, zusätzliche Schutzsysteme anzuschaffen wie Network Access Control. So lässt sich feststellen, wer ins Unternehmensnetzwerk darf und welche Zugriffsrechte er hat – unabhängig davon, mit welchem System er dies macht und von wo aus er zugreifen möchte. Die Eingangstür eines Unternehmens schließt man ja auch ab und lässt nur Mitarbeiter eintreten. Wir raten zusätzlich dazu, im Home Office einen zweiten WLAN-Bereich einzurichten, sodass nur der berufliche Akteur in ein bestimmtes Netz hineinkommt, nicht die ganze Familie.

Idealerweise ist es so, dass die Mitarbeiter den Rechner vorkonfiguriert bekommen und nur noch einstöpseln müssen.

Gibt es rechtliche Fallstricke, die nicht ausreichend beachtet werden?

Einige Regeln haben sich in den letzten Jahren verschärft. Wer beispielsweise kein Backup macht und dann wichtige Daten verliert, kann als Geschäftsführer mit einem Bein im Gefängnis stehen. Das wird mittlerweile von den Steuerprüfern auch nachgefragt. Und wenn das einmal nicht klappt, sinkt man im Ranking der Banken und anderen Institutionen. Das kann sich sehr negativ auswirken.

Was bedeutet die neue Fassung des IT-Sicherheitsgesetzes, das noch in diesem Jahr beschlossen werden soll, für Unternehmen?

Die Vorsorgepflicht wird im neuen Gesetz erweitert. Vorher betraf es wirklich nur die kritischen Unternehmen für die Infrastruktur wie Stadtwerke, Energie und Abwasser. Jetzt soll die Anwendung auf weitere Unternehmen ausgedehnt werden – aber nicht alle. Zum Beispiel muss man Sicherheitsvorfälle dann unbedingt dem Bundesamt für Informationssicherheit melden. Das Gute ist, dass sich durch das Gesetz jetzt viele kritische Betriebe zum ersten Mal intensive Gedanken gemacht und ein Sicherheitskonzept entwickelt haben, das theoretisch sowieso die meisten Unternehmen in schriftlicher Form haben sollten. Auf der anderen Seite führt es auch zu mehr Bürokratismus. Denn in den meisten Fällen wird nur eine Checkliste abgearbeitet, ohne die technische Einrichtung zu prüfen. Wenn zum Beispiel eine Firewall vorhanden ist, wird ein Häkchen gesetzt, aber die Qualität der Umsetzung wird nicht angeguckt. Das kann zu einer gefühlten Sicherheit führen, die trügerisch ist.

www.decoit.de

Das „Handbuch Datensicherheit“ von Prof. Kai-Oliver Detken und Prof. Evren Eren ist beim Kommunal- und Schul-Verlag erschienen. Zielgruppe sind sowohl IT-Nutzerinnen und -Nutzer als auch IT-Verantwortliche.

nexxt-change Unternehmensbörse

Sie suchen einen Betrieb, den Sie übernehmen können, oder einen Nachfolger für Ihr Unternehmen? Sie möchten mit qualifizierten Führungskräften und potenziellen Kandidaten für die Fortführung Ihres Unternehmens in Kontakt treten? Unter **www.nexxt-change.org** können Sie aus einer Vielzahl stets aktueller und anonymisierter Inserate passende Profile auswählen und dann über die Handelskammer Bremen Kontakt aufnehmen. Sie können in den Inseraten recherchieren und selbst kostenfreie Inserate einstellen.

nexxt-change ist eine Internetplattform des Bundesministeriums für Wirtschaft und Energie, des Deutschen Industrie- und Handelskammertages sowie verschiedener weiterer Partner.

Kontakt: Elke Bellmer, Telefon: 0421 3637-402, bellmer@handelskammer-bremen.de

www.nexxt-change.org

ecoFinder – die neue Umwelt-, Energie- und Arbeitsschutz-Datenbank der IHKs

Das „grüne Branchenbuch“ der IHK-Organisation bietet einen bundesweiten und kostenfreien Überblick über Dienstleister, Berater, Hersteller und Händler in der Umwelt-, Energie und Arbeitsschutzbranche. Der ecoFinder unterstützt Unternehmen dabei, ihr Leistungsspektrum zu präsentieren, und hilft bei der Verknüpfung mit Angebotssuchenden. Im Zuge der Corona-Krise wurde die Möglichkeit ergänzt, sich als Hersteller oder Händler von medizinischen Schutzausrüstungen bundesweit und kostenfrei darzustellen.

Kontakt: Franziska Kaufmann, Telefon 0471 3637-364, kaufmann@handelskammer-bremen.de

www.ihk-ecofinder.de

IHK-Recyclingbörse

Suchen Sie neue Verwertungsmöglichkeiten für Ihre Abfälle oder Reststoffe? Benötigen Sie selbst verwertbare Stoffe, um Ihre Anlagen optimal auszulasten? Die Angebote der kostenfreien IHK-Recyclingbörse finden Sie jetzt komplett online.

Kontakt: Andrea Scheper, Telefon 0471 3637-371, scheper@handelskammer-bremen.de

www.ihk-recyclingboerse.de

Impressum

wirtschaft in Bremen und Bremerhaven
102. Jahrgang | April 2021

www.handelskammer-magazin.de

Herausgeber Handelskammer Bremen – IHK für Bremen und Bremerhaven, Am Markt 13, 28195 Bremen, Telefon 0421 3637-0, service@handelskammer-bremen.de, www.handelskammer-bremen.de

Verlag Carl Ed. Schünemann KG, Zweite Schlachtpforte 7, 28195 Bremen, Telefon 0421 36903-72, www.schuenemann-verlag.de

Vertriebsleitung Katrin Greinke, Telefon 0421 36903-44, greinke@schuenemann-verlag.de

Anzeigenleitung Karin Wachendorf, Telefon 0421 36903-26, anzeigen@schuenemann-verlag.de
Es gilt die Anzeigenpreisliste Nr. 6 vom 1. Januar 2021.

Chefredaktion Axel Kölling, wibb@k-ms.de

Ansprechpartner des Herausgebers Dr. Stefan Offenhäuser, Syndicus, offenhaeuser@handelskammer-bremen.de, und Christiane Weiß, Referentin Public Relations, weiss@handelskammer-bremen.de

Konzept, Grafik, Herstellung Carl Ed. Schünemann KG

Druck Druckerei Girzig & Gottschalk GmbH

Preise Einzelheft: Euro 2,50; Jahresabonnement: Euro 12,60
Die beitragspflichtigen Kammerzugehörigen erhalten die „Wirtschaft in Bremen und Bremerhaven“ auf Anfrage kostenlos. Die Zeitschrift erscheint 6 Mal im Jahr. Für unverlangt eingesandte Manuskripte und Fotos übernimmt der Verlag keine Haftung. Nachdruck, auch auszugsweise, ist nur mit Quellenangabe gestattet. Sämtliche Rechte der Vervielfältigung liegen bei der Handelskammer Bremen. Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Handelskammer wieder. Anzeigen- und Redaktionsschluss ist der 6. des Vormonats.
ISSN 2509-3371

Erscheinungsweise bis zum 10. des Monats

Datenschutzhinweis Die personenbezogenen Daten werden auf der Basis der geltenden Datenschutzgesetze, insbesondere der EU-Datenschutzgrundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG), zweckgebunden erhoben und verarbeitet. Wir geben Ihre Daten nur weiter, soweit ein Gesetz dies vorschreibt oder wir Ihre Einwilligung eingeholt haben. Die personenbezogenen Daten sind für die Lieferung Ihrer Ausgabe der „Wirtschaft in Bremen und Bremerhaven“ erforderlich. Unsere Informationen zum Datenschutz nach Art. 13 und Art. 14 der EU-DSGVO können Sie auf unserer Internetseite unter www.schuenemann-verlag.de einsehen oder unter der Telefonnummer 0421-36903-76 bzw. über info@schuenemann-verlag.de anfordern.

ivw geprüft

FSC-Logo
(wird von Druckerei eingesetzt)

Veranstaltungen

Angebot der Handelskammer: Präsenzseminare, webbasierte Seminare – Online-Übersicht

Die Veranstaltungen der Handelskammer, die bisher in einer halbjährlichen Printbroschüre vorgestellt wurden, finden Sie jetzt komplett in der Online-Veranstaltungsübersicht:

www.handelskammer-bremen.de/veranstaltungen

Dort finden Sie eine sehr große und vor allem tagesaktuelle Auswahl an Workshops, Seminaren, Vorträgen und Weiterbildungsangeboten. Viele webbasierte Seminare sind dazugekommen.

Online können Sie aus mehr als 200 Veranstaltungen ein passendes Angebot auswählen und direkt buchen. Zudem können Sie langfristig planen: Die Termine der Online-Angebote decken einen Zeitraum von mehr als zwölf Monaten ab. Eine Stichwortsuche führt Sie zu den gewünschten Themen.

Ein wöchentlicher Handelskammer-Newsletter informiert Sie des Weiteren über Handelskammer-Veranstaltungen. Er kann hier abonniert werden:

www.handelskammer-bremen.de/newsletter