INTERVIEW |

Der Faktor Mensch ist entscheidend

Unternehmen aller Branchen können Opfer von Cyberangriffen werden – umso wichtiger sind konsequente Schutzmaßnahmen. Exemplarisch berichten Matthias Blatz, Geschäftsführer von Heidelberg iT, und Dr. Jens Bortloff, kaufmännischer Leiter des Technoseums, über die Zusammenarbeit in Sachen IT-Sicherheit, die Verantwortung von Vorgesetzten und Digitalität im Museum.

Bild: Sunny studio/stock.adobe.com

Alte Gegenstände in ähnlich historischen Vitrinen – diese Vorstellung von Museum ist längst nicht mehr zeitgemäß, moderne Technik hat auch hier längst Einzug gehalten und spielt bei der Informationsvermittlung eine wichtige Rolle. Wie wichtig ist in diesem Zusammenhang die Informationssicherheit, Herr Bortloff?

Dr. Jens Bortloff: Sehr wichtig. Die Informationssicherheit nimmt zunehmend eine größere Bedeutung ein. Da mittlerweile fast alles, was elektronisch ist, praktisch einen kleinen Computer darstellt und per WLAN Teil des Hausnetzes ist, ist vieles unserer Ausstellung Teil unserer IT. Im Technoseum verfügen wir überall über WLAN, damit betreuen wir auch unsere elektronischen Teile der Ausstellung. Denn moderne Medienstationen spielen eine große Rolle. Zielbewusst eingesetzt, sind diese eine ideale Ergänzung zu den historischen Objekten, Inszenierungen und den beliebten analogen Mitmachstationen unserer Ausstellung.

Herr Blatz, das Beispiel Museum zeigt es: Jedes Unternehmen ist heutzutage mit der Gefahr eines (digitalen) Angriffs konfrontiert – und doch sind die Anforderungen im Hinblick auf die Informationssicherheit individuell unterschiedlich. Wie erkenne ich als Unternehmer überhaupt, welche Schutzmaßnahmen für meine Firma angemessen und hilfreich sind?

Matthias Blatz: Informationssicherheit sorgt für die Sicherheit aller Informationen einer Organisation, die notwendig sind, um die Aufgabe oder das Unternehmensziel der Organisation zu erfüllen. Dazu zählen alle Werte, die mit der Verarbeitung der Informationen in Verbindung stehen. Auch gehören Informationen, Daten und Fachwissen dazu – unabhängig davon, ob sie analog, digital oder in den Köpfen verarbeitet und gespeichert werden. Es gilt, die Risiken nach branchenspezifischen und unternehmensindividuellen Anforderungen zu ermitteln, zu bewerten und mit entsprechenden Sicherheitsmaßnahmen präventiv zu minimieren. Hilfreich und angemessen sind Maßnahmen, die im Sinne des festgestellten Schutzbedarfs die betreffenden Assets ausreichend absichern und die sich zudem mit einem wirtschaftlich darstellbaren Ressourceneinsatz umsetzen lassen.

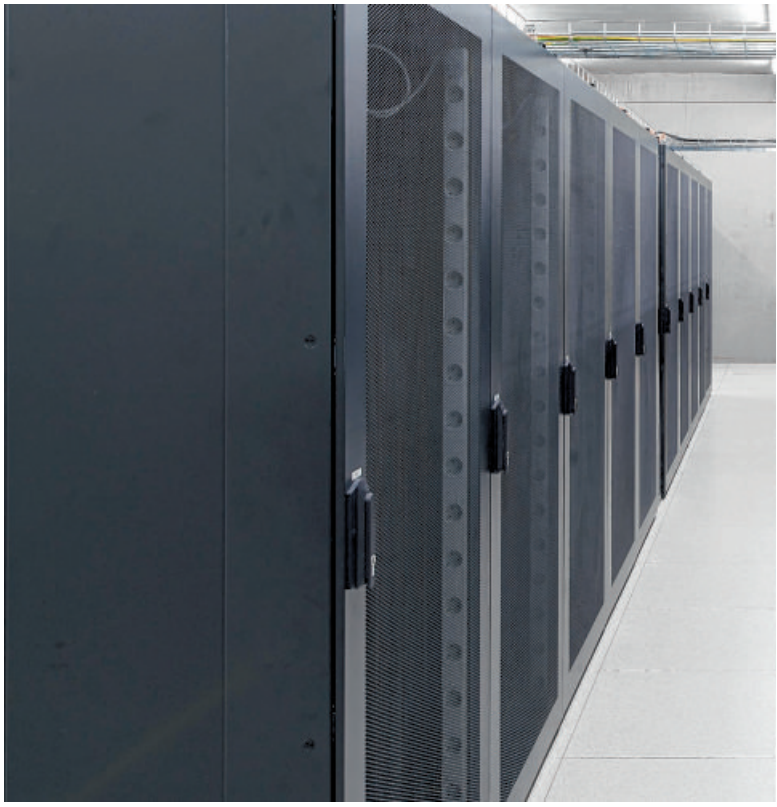
Welche Bedeutung hat die Awareness, die Sensibilität der Mitarbeiter, für den Umgang mit Daten?

Blatz: Allein mit Technik sind Informationssicherheit, IT-Sicherheit und Datenschutz nicht wirkungsvoll durchzusetzen. Der Faktor Mensch ist nach wie vor ein großes Sicherheitsrisiko für Unternehmen. Wir empfehlen daher, Sensibilisierungsmaßnahmen und IT-Sicherheitsschulungen regelmäßig abzuhalten, und zwar für alle betrieblichen Akteure über alle Hierarchieebenen und Standorte hinweg. Wesentlich ist jedoch, dass Unternehmensführung und Fachverantwortliche die Regeln und Vorgaben der Informationssicherheit bei der betrieblichen Arbeit vorleben. Nur so kann die Verankerung der Sicherheitskultur in der Organisation gelingen.

Wie offen sind Unternehmen Ihrer Erfahrung nach dafür, in dieses Thema – technische Ausrüstung, Schulung von Mitarbeitern – zu investieren? Wächst das Bewusstsein dafür?

Blatz: Ja, nach unserer Einschätzung nimmt das Sicherheitsbewusstsein zu und es ist in den Führungsebenen angekommen, dass ein Unternehmen nur dann IT-sicher ist, wenn zeitgemäße Technik eingesetzt wird und alle mitmachen. Schauen wir aber genauer hin, wird im Falle von Mitarbeitersensibilisierung oft erst dann gehandelt und etwa ein externer Dienstleister für Awareness-Schulungen hinzugezogen, wenn es bereits zu einem Sicherheitsvorfall gekommen ist. In Sicherheitstechnologien für einen guten Basisschutz oder um ein höheres Sicherheitsniveau zu erreichen, investieren Unternehmen häufiger, beispielsweise in Lösungen für sichere E-Mail-Kommunikation, E-Mail-Verschlüsselung, E-Mail-Archivierung oder Unified Endpoint Management.

Matthias Blatz führt die Geschäfte bei Heidelberg iT.



Das Mannheimer Technik-Museum setzt in Sachen Sicherheit auf die

Wie genau läuft die Zusammenarbeit zwischen Sicherheitsdienstleister und Kunde, in diesem Falle von Technoseum und Heidelberg iT, konkret ab?
Bortloff: Heidelberg iT ist im Laufe der letzten Jahre ein wichtiger Partner geworden, denn ein immer größerer Teil unserer IT liegt in deren Betreuung. Die Zusammenarbeit besteht darin, dass Heidelberg iT bestimmte Daueraufgaben erledigt, zum Beispiel unser Backup. Zum anderen klärt unser eigenes IT-Team aufkommende Probleme oder Fragen bei Bedarf. Aktuell arbeitet unsere IT gemeinsam mit den Heidelberger IT-Spezialisten am Aufbau und der Umsetzung eines Managementsystems für Informationssicherheit nach der IT-Grundschutz-Methodik des BSI. Heidelberg iT stellt dabei den Informationssicherheitsbeauftragten, der den Sicherheitsprozess steuert. Schließlich berät uns Heidelberg iT bei der ständigen Fortentwicklung der IT-Infrastruktur.

Welche konkreten Schritte sind denn grundsätzlich zur Implementierung geeigneter Schutzmaßnahmen empfehlenswert? Und wie lässt sich die Sicherheit im komplexen Arbeitsalltag, wie im Beispiel des Technoseums, aufrechterhalten? Braucht es dazu eine Art externes Monitoring oder können die Firmen und ihre Mitarbeiter das selbst – gewissermaßen nebenher – gewährleisten?
Blatz: Wir setzen auf einen systematischen, ganzheitlichen Ansatz und empfehlen die Einführung eines Informationssicherheitsmanagementsystems, kurz ISMS. Damit wird die Organisation der Informationssicherheit koordiniert, umgesetzt und kontrolliert. Wichtig ist, dass Informationssicherheit zur Chefsache erklärt wird und die Unternehmensleitung den Sicherheitsprozess initiiert. Im ersten Schritt wird eine Leitlinie erstellt, die Sicherheitsorganisation aufgebaut und Verantwortlichkeiten geschaffen. Es wird ein ISMS-Team aus Experten unterschiedlichster Sicherheitsbereiche im Unternehmen gebildet und ein Informationssicherheitsbeauftragter (ISB) benannt. Er steuert die Einführung, Umsetzung und Aufrechterhaltung des ISMS und koordiniert das ISMS-Team. Wer einen externen ISB wählt, vermeidet mögliche Betriebsblindheit und spart Ressourcen, zum Beispiel müssen intern keine Fachkräfte qualifiziert oder neue gewonnen werden.

„Wichtig ist, dass Informationssicherheit zur Chefsache erklärt wird und die Unternehmensleitung den Sicherheitsprozess initiiert."

Matthias Blatz,
Heidelberg iT

Im bisherigen SWR-Gebäude in Mannheim plant das Technoseum bis 2023 die Eröffnung des Zentrums Digitaler Wandel, einer Institution, die bundesweite Strahlkraft entwickeln soll. Museen als Zeugen und Analysten von Entwicklungsprozessen werden ja eher für den Blick auf Vergangenes herangezogen. Inwieweit bedeutet das neue Zentrum im digitalen Transformationsprozess einen Perspektivwechsel?

Bortloff: Auch die Vergangenheit war einmal Zukunft und Gegenwart, so dass hieraus wertvolle Erkenntnisse für heute und die Zukunft gezogen werden können. Im Technoseum kann man die Geschichte der Industrialisierung anhand vieler Beispiele nachvollziehen. Diese Rückschau betrifft die drei bisherigen industriellen Revolutionen. Wir sind mitten in der vierten – Stichwort „Industrie 4.0" – die wir folgerichtig ebenfalls abbilden und begleiten. Mit

IT-Kompetenz aus der Nachbarstadt am Neckar.

Dr. Jens Bortloff, kaufmännischer Leiter des Technoseums Bilder: oh

dem neuen Zentrum werden wir noch besser die Möglichkeit haben, aktuelle und zukünftige Entwicklungen der digitalen Transformation zu erklären und die Verantwortung für den Umgang mit der Digitalität in den Fokus zu stellen, gerade auch bei Kindern und Jugendlichen. Genau dies mit dem Wissen und dem Hintergrund der historischen Erfahrungen zu tun, bietet das Technoseum.

Stellt der Aufbau des neuen Digitalzentrums im Technoseum auch im Hinblick auf die Herausforderungen bei der Informationssicherheit einen Meilenstein dar? Da müsste es für Heidelberg iT ja viel zu tun geben ...

Blatz: Sicherheit im Kontext des „Zentrums digitaler Wandel" im Technoseum bedeutet die Sicherheit von Räumen, von interaktiven Ausstellungen, Exponaten und nicht zuletzt von Menschen: Personal und Besucher. Um die relevanten Werte zu schützen, muss das Sicherheitsmanagement in die existierenden Managementstrukturen des Landesmuseums eingebettet und an spezifische Gegebenheiten angepasst werden. Eine anspruchsvolle Aufgabe in einem zukunftsweisenden Projekt, die unseren IT-Spezialisten viel Freude macht.

Bortloff: Es ist klar, dass bei der Darstellung und Erläuterung der Digitalität auch digitale Technik eingesetzt wird. Bereits jetzt setzen wir neue Anschauungsmittel ein, wie zum Beispiel „Erweiterte Realität", und werden zukünftig wohl auch Technologien einsetzen, die wir jetzt nur in Ansätzen kennen, etwa künstliche Intelligenz. Hierzu ist es wichtig, dass wir einen verlässlichen Partner wie Heidelberg iT haben, denn unsere digitalen Medien sollen jeden Tag zuverlässig für unsere Besucher funktionieren. *Interview: Moritz Tzschaschel*