Verlagsbeilage, Oktober 2017

‹kes›

Die Zeitschrift für Informations-Sicherheit

special

DS-GVO: Kollision von Anspruch und Realität?

S. 18

Security-Spezialisten: Karrieresprung durch Weiterbildung

ab S. 12

it-sa 2017

Trends, Produkte und Lösungen

DATAKONTEXT

Interview mit Bernd Dieckmann, Director Sales DACH bei Nexus

„Sicherheit gilt immer noch viel zu häufig als notwendiges Übel“

Allgegenwärtige Vernetzung, neue gesetzliche Bestimmungen und immer raffiniertere Cyberattacken: Bernd Dieckmann, Director Sales DACH bei dem IAM-Anbieter Nexus, spricht im Interview über die Notwendigkeit einer umfassenden Sicherheitsstrategie für Unternehmen und Behörden.

Herr Dieckmann, vor welchen Herausforderungen stehen Organisationen derzeit beim Thema IT-Sicherheit?

Nach meiner Einschätzung sind es vor allem vier Themen, die den Bereich IT-Sicherheit aktuell bestimmen. Das erste ist die Digitalisierung, durch die neue Geschäftsmodelle entstehen, die allesamt auf der Nutzung, Analyse und Verarbeitung zunehmend großer Datenmengen basieren und neue Einnahmequellen verheißen. Das zweite ist der digitale Wandel, durch den die Vernetzung zwischen Menschen, Computern, Maschinen und Dingen weiter zunimmt. Durch die Zunahme der digitalen Kommunikationsprozesse und -kanäle wächst jedoch auch die Zahl der potenziellen Sicherheitslücken. Das bringt uns zum dritten Thema: die Cyberkriminalität. Petya, Wannacry und Co. führen uns vor Augen, wie verwundbar Organisationen durch die Digitalisierung geworden sind. Thema Nummer vier sind die neuen gesetzlichen Regularien, die den Herausforderungen der Digitalisierung begegnen sollen. Ein Beispiel hierfür ist die EU-Datenschutz-Grundverordnung, die europaweit einheitliche Maßstäbe in Sachen Datenschutz schaffen will. All das zeigt ganz klar: Unternehmen und Behörden brauchen eine umfassende und gut durchdachte Sicherheitsstrategie, um auch in Zukunft erfolgreich und gesetzeskonform zu sein.

Wo stehen Unternehmen Ihrer Erfahrung nach? Wo sind sie schon aktiv, und wo besteht noch Nachholbedarf?

Cyberangriffe haben in den letzten Jahren hinsichtlich ihrer Reichweite und Wirkung eine ganz neue Qualität erreicht. Dennoch werden Unternehmen bei sicherheitstechnischen Fragen häufig erst dann aktiv, wenn ein Zwang von außen besteht, beispielsweise wenn bei Nichteinhaltung von gesetzlichen Vorgaben Geldstrafen drohen. Und viele Organisationen erkennen Handlungsbedarf leider erst dann, wenn es zu spät ist und sie Opfer eines Angriffs wurden. Besonders kleinere und mittelständische Unternehmen konzentrieren sich oft sehr stark auf ihr Kerngeschäft, weshalb das Thema Sicherheit nicht selten zu kurz kommt und eher als „notwendiges Übel“ denn als Chance für neue Geschäftsfelder betrachtet wird. Gleichzeitig begegnen uns aber auch immer wieder Unternehmen, die das Thema Sicherheit ganz oben auf ihrer Agenda platzieren und konzeptionell in ihrer Unternehmensstrategie verankern. Schließlich wird der Bedarf an benutzerfreundlichen, digitalen und vor allem sicheren Services weiter wachsen.

Welche Rolle spielt im Gesamtkontext IT-Sicherheit das Identitäts- und Access-Management?

Identitäten, insbesondere auch digitale, sind der zentrale Sicherheitsanker eines Unternehmens. Nur durch die Konstruktion verschiedener Identitäten lassen sich die vielfältigen Berechtigungen für Mitarbeiter, Kunden, Lieferanten oder Besucher eines Unternehmens steuern. So entscheiden zugeordnete Identitäten in der physischen Welt darüber, wer Zugang zu bestimmten Räumlichkeiten erhält, während sie in der digitalen Welt den Zugriff auf bestimmte Daten und Systeme regeln. Um beide Welten miteinander in Einklang zu bringen, entscheiden sich immer mehr Organisationen für ein zentral gesteuertes Identitäts- und Zugangsmanagement. Es lässt sich in bestehende Sicherheitsinfrastrukturen integrieren und bietet neben zentralen Richtlinien auch übergeordnete Prozesse. Aufgrund seiner Durchgängigkeit über sämtliche analogen und digitalen Organisationsprozesse hinweg schließt es Sicherheitslücken und ermöglicht eine ganzheitliche

360-Grad-Perspektive zu sicherheitsrelevanten Aspekten. Außerdem reduzieren effiziente Abläufe den administrativen Aufwand um ein Vielfaches; manuelle Prozesse, die fehleranfällig sind und daher häufig großes Risikopotenzial in sich bergen, können durch das System weitgehend eliminiert werden.

Welche Prioritäten sollten Unternehmen bei ihrer IT-Sicherheitsstrategie setzen und wie sehen zukunftsorientierte Sicherheitslösungen aus?

Jedes Unternehmen muss sich klar werden, was der Kern seines Geschäftsmodells ist und wie dieser am besten geschützt werden kann. Wichtig ist hierbei insbesondere die Nutzererfahrung. Denn wenn Mitarbeiter sicherheitsrelevante Prozesse umgehen, weil die Systeme nicht nutzerfreundlich sind, erhöht dies im Zweifelsfall das Risiko noch. Sicherheit ist niemals nur Selbstzweck, deshalb müssen sich die Verantwortlichen in den Unternehmen schon in der Planungsphase überlegen, wie das System flächendeckende Akzeptanz unter den Mitarbeitern findet – etwa durch eine bedienungsfreundliche Oberfläche. Ein weiterer Aspekt ist der Trend zu Sicherheit „as a Service". Daraus ergeben sich gerade für kleine und mittlere Unternehmen neue Möglichkeiten zur Nutzung von Sicherheitslösungen, die zu jedem Zeitpunkt „state of the art" sind und kontinuierlich an veränderte Anforderungen angepasst werden. Zu guter Letzt erkennen wir auch eine wachsende Nachfrage nach PKIs, die ein Höchstmaß an Sicherheit in puncto Authentifizierung bieten. Zu den zentralen Funktionen, die mit einer PKI umgesetzt werden können, gehören eine starke Authentifizierung, Datenverschlüsselung und digitale Signaturen.

Welche Trends spielen eine wichtige Rolle – und welche Antwort hat Nexus darauf?

Bernd Dieckmann ist seit rund 15 Jahren im Bereich Identity- und Access-Management tätig und verantwortet heute als Director Sales DACH den Vertrieb bei der Nexus Technology GmbH. Er verfügt über umfangreiches Know-how in den Themen IT-Sicherheit sowie Physical und Digital Access.

Ein wichtiger Trend ist in jedem Fall das Thema Mobilität. Immer mehr Menschen arbeiten flexibel hinsichtlich Zeit und Ort. Dementsprechend muss der mobile Zugriff auf digitale Ressourcen zuverlässig geschützt werden. Nexus begegnet dieser Entwicklung mit der App „Nexus Personal Mobile", die eine sichere Authentifizierung auf mobilen Geräten bietet. Die App setzt auf PKI-Technologie und kombiniert hohe Sicherheitsstandards mit Benutzerfreundlichkeit. Mit „Nexus Personal Mobile" benötigen Mitarbeiter kein Passwort mehr, um sich sicher an Cloud- und Online-Services anzumelden. Für die Authentifizierung kann beispielsweise der Fingerabdrucksensor des Smartphones verwendet werden, was zusätzliche Identitätsträger wie Hardware-Token obsolet macht.

Wie positioniert sich Nexus im Markt für IT-Sicherheitslösungen?

Nexus beschäftigt sich seit über 30 Jahren mit dem Identitäts- und Zugangsmanagement. Was uns wohl vor allem auszeichnet, ist die Kompetenz, in diesem Thema die 360°-Grad-Perspektive einzunehmen und die physische und die digitale Welt durch die Bereitstellung zukunftsfähiger Sicherheitslösungen zusammenzuführen. Auf diesem Gebiet sind wir Profis und blicken auf viele erfolgreiche Projekte zurück. Zu unseren Kunden zählen Global Player ebenso wie Mittelständler und Behörden. Was uns jedoch vor allem prägt, ist unser Wertesystem, an dem wir uns intern und in der Zusammenarbeit mit unseren Kunden und Partnern orientieren. Dieses System leben wir durch Wertschätzung und einen partnerschaftlichen Umgang – und ohne das wäre unser Erfolg so nicht denkbar. ■

Messestand: Halle 10.0, Stand 320