neXus: Sechs Themen treiben Identitätsmanagement in 2016

Ettlingen, xx. Januar 2016 – Für neXus, führender internationaler Anbieter von Sicherheitslösungen und -dienstleistungen, wird Identitätsmanagement 2016 zu einem der zentralen Themen im Kontext von IT-Sicherheit. Verantwortlich dafür sind Trends wie die anhaltende Flexibilisierung der Arbeitswelt, neue Formen der Kundenkommunikation und die wachsende Zahl an Cyberangriffen.

Die digitale Transformation eröffnet Unternehmen ebenso wie Behörden neue Perspektiven: Sie optimieren ihre Prozesse und setzen damit interne Kapazitäten frei, sie senken ihre Kosten, nutzen neue Kanäle für den Dialog mit Kunden und Bürgern und gestalten ihre Produktion flexibler. Um die Sicherheit der dahinter stehenden Prozesse zu gewährleisten, ist ein durchgängiges und zuverlässiges Identitätsmanagement jedoch unerlässlich. Folgende Trends in diesem Jahr werden die Nachfrage nach entsprechenden Lösungen 2016 besonders stark treiben:

- **Cyberangriffe:** Die Zahl der Cyberangriffe wächst permanent, und sie werden immer raffinierter und komplexer. Allein für die deutsche Wirtschaft wird der finanzielle Schaden auf 50 Milliarden Euro pro Jahr geschätzt. Datendiebstähle riesigen Ausmaßes rund um den Globus machen immer wieder Schlagzeilen; zudem bringt die fortschreitende Vernetzung und Digitalisierung nicht zuletzt das Risiko mit sich, dass das gesamte Wissen eines Unternehmens auf einen Schlag gestohlen oder zerstört werden kann. Gleichzeitig bemerken viele Unternehmen Manipulationen ihrer Systeme gar nicht – oder erst, wenn es zu spät ist. Deshalb benötigen neben natürlichen Personen auch alle Objekte oder Ressourcen, die im Rahmen eines Netzwerks „kommunizieren“ (beispielsweise Server, Applikationen, Maschinen, mobile Endgeräte) eine zweifelsfreie Identität, um sich als sichere und vertrauenswürdige Komponenten und Quellen auszuweisen. Zusätzlich gilt es, den digitalen Kanal mit Hilfe von Verschlüsselungen vor Angriffen von außen zu schützen.
- **Industrie 4.0 / Internet of things**: Die Verschmelzung traditioneller Industrien mit der IT unter dem Label Industrie 4.0 / IoT lässt die Zahl an Identitäten sprunghaft ansteigen (siehe oben). Wenn produzierende Unternehmen ihre Prozesse absichern wollen, müssen diese allesamt zweifelsfrei definierbar sein, sich ausweisen können und effizient verwaltet werden. Gleichzeitig müssen die Unternehmen auch den physischen Zugang zu Maschinen, aber auch zu ganzen Produktionsbereichen eindeutig und sicher regeln, um Manipulationsrisiken auszuschalten.
- **Flexibilisierung der Arbeitswelt**: Unsere Arbeitswelt ist in den letzten Jahren immer flexibler geworden; die Zusammenarbeit mit Dienstleistern und freien Mitarbeitern, Projektarbeit, aber auch flexible Arbeitszeitgestaltung der eigenen Mitarbeiter gehört längst zum Alltag. Immer mehr Mitarbeiter loggen sich zudem über mobile Geräte in die Systeme ihres Arbeitgebers ein. Klare Regeln für den Zugriff auf Daten und Systeme und die Schaffung ihrer technischen Voraussetzungen sind vor diesem Hintergrund unerlässlich.
- **Neue digitale Geschäftsmodelle**: Aus Big Data wird für immer mehr Unternehmen eine begehrte Ressource, und dazu zählen längst nicht mehr nur die allseits bekannten Internet-Giganten. Konzepte wie “connected cars” verändern die Beziehung zwischen

Anbieter und Nutzer, und immer mehr Unternehmen entwickeln neue Konzepte für einen direkten Kundenkontakt über digitale Kanäle. Ohne ein zuverlässiges Management von Identitäten und Berechtigungen werden derartige Geschäftsmodelle schon im Ansatz scheitern.

- **Wachsendes Bewusstsein für Sicherheitsrisiken im öffentlichen Sektor**: Der staatliche Sektor ist von Cyberattacken in besonderem Maße betroffen, denn längst ist das Internet nicht nur zum Schauplatz von Wirtschaftskriminalität, sondern auch zur Kampfarena zur Erreichung politischer, aber auch terroristischer Ziele geworden. Laut dem Cyber-Sicherheitsrat e.V. besitzen oder entwickeln rund 150 Staaten digitale Angriffs- oder Verteidigungswaffen. Die Sensibilität für Sicherheitsrisiken und die Investitionsbereitschaft ist im öffentlichen Sektor gestiegen; Lösungen für ein umfassendes Identitätsmanagement werden dabei zunehmend als integraler Bestandteil einer umfassenderen IT-Sicherheitsstrategie angesehen.
- **Schutz kritischer Infrastrukturen:** Terroranschläge und Naturkatastrophen, aber auch Systemausfälle wie in Fukushima haben das Bewusstsein für die Verwundbarkeit so genannter kritischer Infrastrukturen gestärkt. Zu diesen zählen Organisationen und Einrichtungen, die für das Funktionieren des Gemeinwesens von zentraler Bedeutung sind, also unter anderem Energieversorger, die DB Bahn und große Banken. Bereits heute schreibt der Gesetzgeber diesen systemrelevanten Organisationen alle zwei Jahre ein Sicherheitsaudit vor und verpflichtet sie zur kontinuierlichen Optimierung ihrer Sicherheits-Infrastruktur. Die zunehmende Interdependenz der einzelnen Sekoren und der Einsatz von IT-Technologien (Stichwort Smart Grids) erfordert zukünftig noch umfassendere und modernere Schutzmaßnahmen.

Unternehmen praktisch aller Branchen ebenso wie Behörden müssen demnach mehr Sensibilität für Security-Themen entwickeln, wenn sie ihr Geschäftsmodell nicht gefährden und die Potenziale der Digitalisierung auch wirklich nutzen wollen – und sie müssen diesem Bewusstsein Taten beziehungsweise Investitionen folgen lassen. „Unternehmen und staatliche Institutionen sollten IT-Sicherheit als Asset betrachten, das das eigene Geschäftsmodell für die Zukunft absichert und damit auch Reputation schafft bei den Zielgruppen“, kommentiert Bernd Dieckmann, Geschäftsführer bei neXus.
neXus berät und entwickelt flexible Sicherheitslösungen für Unternehmen zahlreicher Branchen sowie Behörden, und ist mit seinem Lösungsportfolio optimal für den aktuellen Bedarf im Markt gerüstet. Das Unternehmen bietet über die Bereitstellung eines zentralen Systems für das Identitäts- und Access-Management branchenübergreifend einheitliche Richtlinien bei der Verwaltung von Identitäten, Credentials und Berechtigungen, und maximalen Schutz angesichts der zunehmenden Digitalisierung von Prozessen.

Über neXus
neXus ist ein führender internationaler Anbieter von IT-Sicherheitslösungen und -dienstleistungen im Bereich Physical und Digital Access Management. Ein umfangreiches Angebot macht neXus zu einem idealen Provider für Identity- und Access Management-Lösungen aus einer Hand. neXus hat Niederlassungen in Deutschland, Schweden, Norwegen, Dänemark, Finnland, Frankreich, Indien und Großbritannien. Weitere Informationen finden Sie unter www.nexusgroup.com.

Pressekontakt:
Claudia Wittwer
Burson-Marsteller GmbH
Claudia.Wittwer@bm.com
+49 (0)89-17319440