die Ansicht, dass Angriffe, die auf den Diebstahl privilegierter Zugangsdaten zurückzuführen sind, am schwierigsten zu entdecken und zu beheben sind. Nur 29 % nannten hier Malware und lediglich 11 % die Überwindung des Perimeter-Schutzes.

Auf die Frage, welche Cyber-Attacken oder Insider-Angriffe des letzten Jahres maßgeblich zu einer Veränderung der eigenen Sicherheitsstrategie beigetragen haben, nannten:

- 37 % die NSA/Edward Snowden-Affäre
- 31 % Cyber-Angriffe wie PoS-Attacken
- 19 % Spionageaktivitäten von Regierungen

Da immer mehr Unternehmen Cloud-Services nutzen oder externen Providern einen Netzwerkzugriff erlauben, werden auch diese Dienstleister zunehmend zum Ziel von Cyber-Angreifern. Die Gefahr wird überaus deutlich, wenn man bedenkt, dass 60 % der Befragten Externen eine Remote-Zugriffsmöglichkeit auf ihr internes Netzwerk einräumen. Über die Hälfte (58 %) ist sich dabei nicht sicher, ob ihr Service Provider privilegierte Accounts schützt und überwacht. Gelangt ein Angreifer in den Besitz der Zugangsdaten, kann er problemlos auf Kunden-Unternehmensnetzwerke zugreifen.

Ein weiteres Ergebnis der CyberArk-Untersuchung ist, dass die Einführung neuer Sicherheitsstrategien nicht nur durch das steigende Bedrohungspotenzial, sondern auch durch neue Trends, Technologien oder regulatorische Anforderungen forciert wird. Genannt wurden hierzu:

- 30 % Bring Your Own Device (BYOD)
- 26 % Cloud Computing
- 21 % Compliance-Richtlinien
- 16 % Internet of things

„Imageschaden, Verlust von Kunden oder finanzielle Einbußen: Das sind nur einige Auswirkungen, mit denen Unternehmen nach Insider-Angriffen oder Cyber-Attacken zu kämpfen haben", betont Jochen Koehler, Regional Director DACH bei CyberArk in Heilbronn. „Unsere diesjährigen Untersuchungsergebnisse haben ganz klar gezeigt, dass das größte Sicherheitsrisiko von privilegierten Benutzerkonten und Zugangsdaten ausgeht. Geraten sie in die falschen Hände, sind Angreifern quasi Tür und Tor zu den vertraulichsten Systemen und Datenbeständen eines Unternehmens geöffnet."

„Immer mehr Unternehmen erkennen das auch", so Koehler weiter, „und implementieren Lösungen im Bereich Privileged Account Security, mit denen sie privilegierte Zugriffe auf beliebige Zielsysteme zentral berechtigen, jederzeit kontrollieren und revisionssicher auditieren können."

Die vollständige CyberArk-Studie kann unter *www.cyberark.com/contact/global-advanced-threat-landscape-survey-2014* angefordert werden.

Softwareentwickler brauchen sichere Bausteine

Eine Analyse des European Center for Security and Privacy by Design in Darmstadt (EC SPRIDE) beschreibt Trends in der Softwareentwicklung und deren Bedeutung für die IT-Sicherheit. Größte Herausforderungen für die IT-Sicherheit sind das zunehmende Entwicklungstempo und die steigende Komplexität von Software.

Unternehmen mit ihren oft weltweit verteilten Entwicklerteams reagieren darauf mit agilen Methoden und vorgefertigten Softwarebausteinen. Um hierbei auch in Zukunft ausreichende IT-Sicherheit zu gewährleisten, wünschen sich Experten automatische Testwerkzeuge sowie die Einbettung von entsprechenden Analysewerkzeugen in Entwicklungsumgebungen. Die Ergebnisse basieren auf Interviews mit Softwareentwicklern und IT-Sicherheitsexperten aus Industrie, Wissenschaft und Behörden. Der Trendbericht steht unter *www.ec-spride.de* zum kostenlosen Download bereit.

Früher dauerte die Entwicklung einer Anwendung oft mehrere Jahre, heute entwickeln Programmierer Apps in wenigen Wochen. Angesichts der großen Beschleunigung der Entwicklungsprozesse verwundert es nicht, dass in den Nachrichten immer wieder Meldungen über schwerwiegende Sicherheitslücken auftauchen. Wissenschaftler am Darmstädter IT-Sicherheitszentrum EC SPRIDE befragten deshalb 23 Experten aus Softwareentwicklung und IT-Sicherheit dazu, wie sich die Entwicklungsprozesse verändern und welche Herausforderungen und Handlungsempfehlungen im Hinblick auf die IT-Sicherheit sich daraus ergeben.

Zu den Ergebnissen der Studie gehört, dass Softwareentwicklung immer flexibler wird: Heutige Entwicklerteams sind oft über den ganzen Globus verteilt und werden ergänzt durch externe Projektpartner, die kommen und gehen. Agile Entwicklungsmethoden begrenzen den bürokratischen Aufwand und sorgen so für große Dynamik. Um ausreichende IT-Sicherheit zu gewährleisten, müssen diese Methoden aber um Sicherheitsprozesse ergänzt werden, die für angemessene Security-Kompetenz über den gesamten Lebenszyklus einer Anwendung sorgen. Dies ist zum Beispiel besonders wichtig, wenn Entwickler das Projekt verlassen und neue eingearbeitet werden müssen. Darüber hinaus raten die Experten dazu, stärker in die Kommunikation innerhalb der Teams investieren.

Außerdem ist eine Demokratisierung der Softwareentwicklung zu beobachten. Selbstlernende Entwicklungsplattformen und Code-Generatoren sorgen dafür, dass auch Menschen ohne umfangreiche und formale Entwicklerausbildung Software erzeugen können. Damit die IT-Sicherheit nicht darunter leidet, müssen Entwicklerteams in die Lage versetzt werden, sachlich begründete Sicherheitsentscheidungen zu treffen. Dabei können verschiedene Dinge helfen, etwa das Einbetten von Sicherheitsfunktionen in Entwicklungsplattformen, die Sicherheitszertifizierung von ganzen Frameworks oder die Entwicklung von automatisierten Testverfahren, verlässlichen Indikatoren für IT-Sicherheit und sicheren Softwarebausteinen.

Online-Payment: Security versus Usability

Immer mehr Menschen kaufen im Internet ein – komfortabel und unkompliziert. Ein Dilemma ergibt sich oft erst beim Bezahlen. Sicherheit und Schnelligkeit sind für Händler wie für Kunden gleichermaßen entscheidend für die Wahl der Bezahlmethode. Die Sicherheit von elektronischen Zahlungen im Onlinehandel soll durch eine stärkere Authentifikation erhöht werden, so die Empfehlung von SecuRe Pay (European Forum on the Security of Retail Payments) unter dem Vorsitz der EZB, welche bis zum 01.Februar 2015 umgesetzt werden soll. EHI-Online-Payment-Experte Tim Kiesewetter warnt davor, dass zu komplexe Autorisierungsmethoden die Bedienbarkeit für den Kunden einschränken und sich dadurch negativ auf den Onlinehandel auswirken: „Was für Mitglieder des Forums unbedingt notwendig erscheint, kann den Kunden leicht überfordern. Die Herausforderung besteht darin, Sicherheit auf der einen Seite mit Einfachheit und Verständlichkeit auf der anderen Seite in Einklang zu bringen."