

Vielfältige Security-Ansätze führen zum Flickenteppich

Die Entscheidung für die richtigen Sicherheitstools fiel den Verantwortlichen noch nie so schwer wie heute. Unterschiedliche Produktstrategien und unklare Begriffe erschweren die Wahl.

Von Hadi Stiel*

Die IT-Sicherheit steht, trotz oder gerade wegen der Wirtschaftskrise, weiterhin im Fokus der Entscheider. Vor allem der Zugriffsschutz soll die IT und darüber das Geschäft der Unternehmen vor Ausfällen und Verlusten bewahren, also wettbewerbsfähig erhalten. Auf der anderen Seite ist kein IT-Markt so stark fragmentiert wie der für IT-Sicherheit. Dementsprechend sind die meisten Sicherheitsstrategien und Produkte, mit denen die Hersteller ihren Kunden einen verlässlichen Zugriffsschutz verheißen, gesplittet.

Norbert Drecker, Geschäftsführer des Sicherheitsberatungs- und -dienstleistungshauses Twinsec, sieht drei generelle Stoßrichtungen: „Die einen, meist kleinere oder mittelgroße Hersteller, konzentrieren sich auf Teillösungen, die mehr oder weniger gut in übergeordnete Sicherheitsansätze großer Hersteller passen. Die anderen versuchen den Sicherheitsmarkt Bottom-up vom Netz aus aufzurollen.“ Eine dritte Herstellergruppe gehe die Zugriffskontrolle Top-down an, ausgehend von den Geschäftsprozessen und den daran beteiligten Applikationen und Usern. „Alle drei Herstellergruppen operieren teils mit denselben Begriffen, obwohl ihre Strategien, Produkte und Funktionen stark differieren“, stellt Drecker fest.

Uneinheitlich verwendet werden etwa die Bezeichnungen Authentifizierung be-

ziehungsweise Authentifizierung, Authentifizierungsverfahren, Autorisierung, Rechteverwaltung, Auditing und Sicherheits-Management. Bernd Redecker, Head of Security Solutions, Professional Services bei Wincor Nixdorf, empfiehlt: „In diesem Zusammenhang sollten Begriffe wie Authentifizierung respektive Authentifizierung nur dann verwendet werden, wenn damit der kontrollierte Zugang zum Beispiel zum betreffenden LAN gemeint ist.“ Die Authentifizierung biete lediglich einen generellen Eingangsschutz, nicht mehr. Erst die gesonderte Autorisierung gegenüber den Applikationen sichere ab, wer mit welchen Anwendungen und Daten arbeiten dürfe. „Diese Trennung verhilft zudem dazu, die richtige Entscheidung für die Stärke der Authentifizierung – Login/Passwort, Token, Chipkarte mit PIN oder, noch sicherer, mit Zertifikat oder biometrischen Informationen – zu treffen“, erklärt Redecker.

Der Kontext zählt

Für den Fall, dass über Single-Sign-on (SSO) der Netzeingangsschutz automatisch mit der Zugriffskontrolle gekoppelt werden soll, empfiehlt Redecker, mindestens auf Tokens zurückzugreifen. „Mit Überwindung einer zu niedrigen Authentifizierungshürde bei SSO würden ansonsten dem Angreifer alle Applikationen offenstehen, für die der rechtmäßige Benutzer vom Administrator autorisiert



Foto: © Alina Iakovitch - Fotolia.com

wurde“, warnt er. Zugriffssicherheit ist weder über die bloße Nutzung von Authentisierungsprotokollen wie Remote Authentication Dial-in User Service (Radius) oder Terminal Access Controller Access Control System (Tacacs+) noch allein über eine hohe Authentisierungsstärke erreichbar. Der Schutz der Autorisierung der Applikationen entscheidet letztlich über die Zugriffssicherheit. Sie kann – ob ohne oder mit SSO – nicht nur klassisch über Login/Passwort, sondern auch über Zertifikat oder biometrische Daten geschaffen werden. Allerdings zieht eine vollständige Integration von Authentisierung und Autorisierung für den Anwender, beispielsweise in Form einer Public-Key-Infrastruktur (PKI), erhebliche Anschaffungs- und Integrationskosten nach sich. Sie sollten der erhöhten Sicherheit gegenübergestellt werden.

Nachteile netzlastiger Strategien

„Die Zeit ist reif, die IT-Sicherheit nicht länger Bottom-up, sondern Top-down von den Geschäftsprozessen aus anzugehen“, sagt Erwin Schöndlinger, Geschäftsführer von Evidian Deutschland. Er wendet sich damit gegen netzlastige IT-Sicherheitsstrategien. Auch die Kopplung der Authentisierung und weiterer Security-Mechanismen mit Netzsystemen wie Routern und Switches und so genanntes Policy-Management hätten sich für die Anwender als „nicht zielführend“ erwiesen. „Solche Strategien haben in den Unternehmen zu einem teuren, löchrigen Flickenteppich meist nicht interoperabler Teilsysteme geführt“, kritisiert der Geschäftsführer. Komplet und von zentraler Stelle ließe sich die Zugriffskontrolle nur überwachen, verwalten und steuern,

Security-Ansätze

Derzeit werden im Wesentlichen drei unterschiedliche Vorgehensweisen diskutiert:

- **Teillösungen** sind eine Domäne kleiner und mittlerer Hersteller. Problematisch ist die Integration in andere Ansätze.
- **Bottom-up:** Diese Ansätze gehen von der Netzebene aus. Meist steht die Kontrolle des Netzwerkzugangs im Vordergrund.
- **Top-down:** Verfechter dieser Idee setzen auf dem Applikations-Layer an. In der Security-Bewertung steht die Anwendung an erster Stelle.

Trendthema IAM

Mit der stärkeren unternehmensübergreifenden Zusammenarbeit (**Collaboration**) setzt sich die Erkenntnis durch, dass die **bisherigen Security-Modelle** nicht mehr greifen. Im Zuge des Paradigmenwechsels wird nun die Idee des Identity- und Access-Managements propagiert. Im **Fokus** steht dabei der Schutz der geschäftskritischen **Anwendungen** und **Prozesse**. Erst im zweiten Schritt werden dann die erforderlichen Authentifizierungsverfahren eruiert und bewertet. Die Verfechter dieses Verfahrens sind davon überzeugt, dass man so der **wachsenden Endgerätevielfalt** (Stichwort Smartphones, Netbooks etc.), neuen Anwendungen (etwa Presence, Videoconferencing) sowie der wachsenden Mobilität **besser gerecht** werde als mit den bisherigen Sicherheitsstrategien.

wenn Identity- und Access-Management (IAM) zum Zuge kommen, so Schöndlinger weiter. IAM setze über seine Module den Zugriffskontrollhebel über Privilegien unterschiedlicher Stärke bei den geschäftsprozesstragenden Applikationen an. Erst im zweiten Schritt müsse Top-down jeweils das angemessene Authentifizierungsverfahren ausgewählt werden.

Sabine Erlinghagen, Leiter des weltweiten Geschäfts mit Identity-Management sowie Biometrie bei Siemens IT Solutions and Services, glaubt ebenfalls an den Top-down-Ansatz. „Die wachsende IT-Durchdringung in den Unternehmen und die Einbindung von Auftraggebern, Geschäftspartnern und Lieferanten ins Netz“ sind ihrer Ansicht nach gute Argumente. Nur über IAM sei es möglich, einheitliche, mit den Partnern abgestimmte Sicherheitsrichtlinien zu kreieren, umzusetzen und danach wirtschaftlich zu verwalten. „Das gilt für die Autorisierung, Authentisierung, Administration der IT-Benutzer und ihrer Rechte und Rollen sowie das Auditing und Reporting gleichermaßen“, unterstreicht Erlinghagen. Eine umfassende Strategie und IAM-Lösung seien somit weit besser als viele in der Summe lückenhafte und nicht strategisch steuerbare Einzelsysteme. Ein Garant dafür sei ein umfassendes IAM-System, das Identity Federation einschließe. Diese Technik Sorge für die notwendige Sicherheit bei der unternehmensübergreifenden Zusammenarbeit und stelle ein Vertrauensverhältnis zwischen den Partnern her, wie komplex das System auch immer sein möge.

Geschäftsführer Drecker von Twinsec sieht spätestens durch die Integration von Sprache und Video via IP sowie mobilere Mitarbeiter das Ende separater oder falsch aufgehängter Sicherheitsansätze und -systeme in großen Schritten nahen. „Die daraus resultierende Applikations-,

Server- und Endgerätevielfalt sowie der Zuwachs an Bewegungsfreiheit können nur ganzheitlich, also unter der Führung von IAM, gemanagt werden“, ist er überzeugt. Wer stattdessen auf viele herstellerspezifische Teilsysteme zur Authentisierung, Autorisierung, Rechteverwaltung, Verschlüsselung, zum Mitschnitt und Sicherheits-Management setze, werde mit der Zeit die Kontrolle über die eigene IT und somit das Unternehmensgeschäft verlieren, warnt Drecker. Er verweist auch auf Gefahren durch die unkoordinierte Flut an Updates sowie vergessene Aktualisierungsläufe.

Zusammenarbeit ist Trumpf

Alexander Wurdack, Mitglied der Geschäftsführung von Logica in Deutschland und Managing Director Outsourcing Germany, sieht nicht nur die Anwender, sondern auch die Outsourcer auf dem Weg zum ganzheitlichen IAM: „Sie sind gefordert, ihre IT-Dienste konzeptionell wie technisch an den Geschäftsprozessen ihrer Kunden und an den daran beteiligten Mitarbeitern auszurichten.“ Outsourcer müssten sich so weit wie möglich von fragmentarischen Sicherheitswerkzeugen, die vor allem auf Netzebene operierten, trennen. Wurdack verweist auf eine Studie, die Logica mit der Outsourcing Unit der London School of Economics (LSE) erarbeitet hat. Wichtige Ergebnisse daraus: Risiken und Gewinne müssen künftig fair zwischen den Vertragspartnern aufgeteilt werden. Die Zusammenarbeit muss sich vom bloßen Vertragsmanagement hin zu einer gemeinschaftlichen Führung der IT entwickeln. IT-Innovationen müssen gemeinsam vorangetrieben, notwendige IT-Veränderungen gemeinsam angepackt werden. ◀

*Hadi Stiel

ist freier Journalist in Bad Camberg.