Höhere IT-Sicherheit durch Privileged Access Management (PAM) der neuen Generation

In jedem Unternehmensnetz gibt es IT-Nutzer mit erhöhten Berechtigungen. Dazu gehören Mitarbeiter der hauseigenen IT-Abteilung, die Zugriff auf sensible Daten und Applikationen haben, aber auch Administratoren von externen IT-Dienstleistern, die im Auftrag von Kunden Rechner und Netzwerksysteme verwalten.

Kein Wunder, dass es Hacker vor allem auf Nutzerkonten von solchen Usern abgesehen haben. Denn wenn es einem Angreifer gelungen ist, einen solchen Privileged Account zu kapern, stehen ihm alle Türen offen. Er kann sich im Unternehmensnetz frei bewegen und in aller Ruhe geschäftskritische Daten stehlen. Nach Erfahrungswerten von IT-Sicherheitsunternehmen dauert es häufig über 100 Tage, bis ein solch gut getarnter Angriff auffällt.

Die Lösung:
Aktivitäten von Nutzen einbeziehen
Einen Ausweg bieten PAM-Lösungen der neuen Generation. Sie beschränken sich nicht darauf, die Identität eines IT-Nutzers zu prüfen, vielmehr bieten sie Funktionen, welche die Aktivitäten des Users berücksichtigen. Eine solche Lösung orientiert sich nicht nur daran, wer der IT-Nutzer ist, sondern auch daran, was er tut.

Ein Element der Lösung ist daher „Privileged Account Analytics“. Diese Funktion erlaubt ein Monitoring der Aktionen eines Privileged Users. Alle Aktivitäten werden in Echtzeit erfasst und analysiert. Das gilt vor allem für verdächtige oder riskante Verhaltensweisen. Wenn z. B. Geschäftsdaten an eine unbekannte E-Mail-Adresse versendet werden oder sein Account plötzlich in der Nacht aktiv ist. Das kann darauf hindeuten, dass nicht der legitime Nutzer, sondern ein Angreifer das Konto nutzt.

User-Sessions unter Kontrolle: Privileged Session Management

Das zweite Element einer PAM-Lösung der neuen Generation ist das Privileged Session Management. Es integriert Funktionen für die Authentifizierung („Bist Du ein legitimer Nutzer?“) und ermöglicht die Autorisierung („Auf welche Server und Anwendungen darfst Du zugreifen?“) von Privileged Usern, welche sich aufgrund ihrer erhöhten Rechte herkömmlicherweise jenseits der aufgestellten Regeln bewegen. Wichtig ist, dass die Lösung alle gängigen Authentifizierungsverfahren und entsprechende Protokolle in den Zugriffsprozess einbindet, etwa Active Directory, LDAP und Radius.

Somit werden Nutzer nicht in ihrer gewohnten Arbeitsweise beeinträchtigt. Außerdem sollten sich für jeden User oder ganze Nutzergruppen Zugriffsrechte („Access Policies“) festlegen lassen.

Bei verdächtigen Vorgängen, etwa einem Verstoß gegen Regeln, erhält das IT-Sicherheitsteam eine Meldung. Zudem werden besonders gefährliche Aktionen umgehend automatisch gestoppt, beispielsweise nach Eingabe eines Löschbefehls.

Ein weiterer wichtiger Aspekt des Privileged Session Management ist das Protokollieren der Sitzungsaktivitäten. So lassen sich bei Sicherheitsvorfällen sowie Systemausfällen schnell Ursachen ausfindig machen um den Normalbetrieb wiederherzustellen.

Information Security

Controlware Security-Portfolio

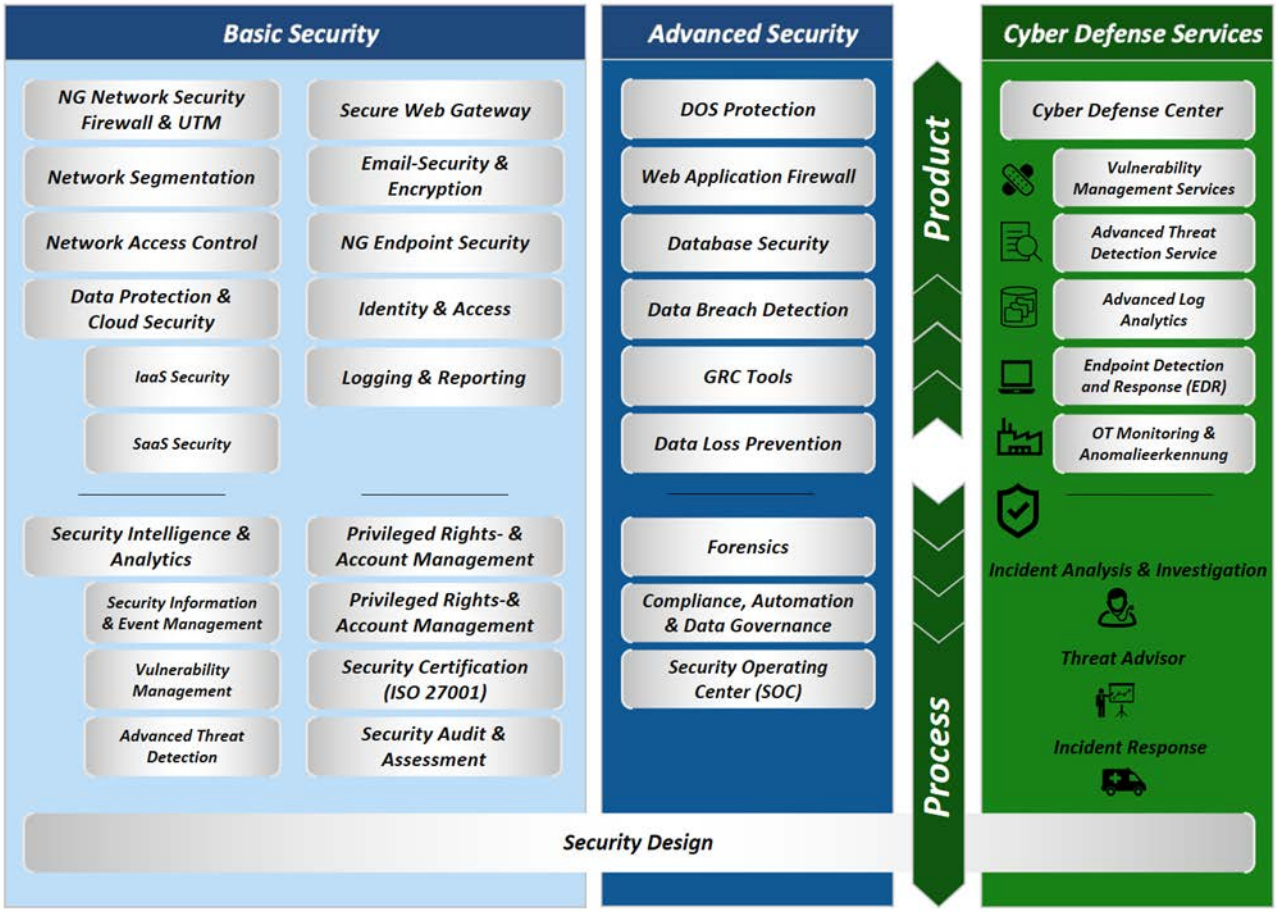
Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Ein vernünftiger Informationsschutz sowie die Grundsicherung von IT und OT sind schon mit verhältnismäßig geringen Mitteln zu erreichen. Informationssicherheit sollte allerdings als laufender Prozess mit Risikoanalyse und Prozessoptimierung verstanden werden um zielgerichtet und möglichst wirtschaftlich in ein Unternehmen oder eine Behörde integriert zu werden.

Die Kombination unserer langjährigen Expertise (Controlware Security seit 1996) mit marktführenden Anbietern von Security-Lösungen steht für erfolgreiche Projekte.

Zusätzlich verschafft uns der höchste Partnerstatus von Controlware bei nahezu allen unseren etablierten Hersteller-Partnern zahlreiche Vorteile, die wir gerne an Sie weitergeben.

Selbstverständlich können Sie auch bei Audits und Zertifizierungen gemäß national und international anerkannter Standards wie ISO 27001, ISO27001 auf Basis IT-Grundschutz / Cobit auf uns bauen.

Mit unseren Controlware Cyber Defense Services erhalten Sie für Ihr Unternehmen modular passende Security Services und mit konkreten Handlungsempfehlungen von unseren erfahrenen Analysten, die zu Ihrer Infrastruktur passen



Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de