ADVERTORIAL

Netzwerk durch lückenloses Access-Management schützen

Wenn externe Dritte auf das eigene Klinik-Netzwerk zugreifen dürfen, ist das eigentlich eine gute Sache.

Dirk Wahlefeld,, Manager Unimate Tech Services, Imprivata GmbH, Langenfeld

Foto: Imprivata

Dirk Wahlefeld

Die Behandlungskette läuft wie am Schnürchen, wenn Zuweiserärzte, Belegärzte und externe Gesundheitsdienstleister, wie Labore, Reha-Einrichtungen oder Pflegedienste, direkten und sicheren Zugriff auf für sie freigegebene Daten aus der Klinik haben. Soweit, so gut – aber nur dann, wenn die Zutrittskontrolle, das Access-Management, funktioniert. Daran hapert es branchenübergreifend, wie eine aktuelle Studie zeigt.

Das Ponemon Institut und Imprivata haben eine internationale Studie zum Thema „Gefahrenquelle Lieferkette" durchgeführt. In Deutschland haben 573 IT-Verantwortliche aus verschiedenen Branchen, u.a. dem Gesundheitswesen und dem öffentlichen Sektor, teilgenommen. Die Ergebnisse, die hier nur auszugsweise vorgestellt werden, sind für die Klinik-IT interessant, wenn auch nicht als repräsentativ anzusehen.

Keine Strategie, aber weitreichende Rechte

Die Einbindung Externer in das Krankenhaus-Netzwerk ist unverzichtbar und mittlerweile gang und gäbe. Belegärzte, Labore und andere Beteiligte der Behandlungskette sollen im Sinne einer optimalen Patientenversorgung z. B. Dokumente hoch- und runterladen können, Anwendungen nutzen und Informationen einsehen. Doch bei der Rechtevergabe toppt meist Pragmatismus die (fehlende) Strategie: 58 % haben keine einheitliche Strategie für die Verwaltung von Zugängen und Berechtigungen für Externe. Die Quittung: Stattliche 51 % der Befragten sagten, dass ihre Organisation in den letzten zwölf Monaten von einer Datenverletzung oder Cyberattacke betroffen war, die von außen ausgeführt wurde. Auf die Frage, warum das möglich war, nannten 34 % als einen Grund, dass Externen zu weitreichende Zugriffsrechte eingeräumt waren. Das wäre noch kein Problem, denn manchmal sind umfangreiche Rechte im Sinne der Prozessoptimierung notwendig.

Vertrauen ist gut, Kontrolle und Doku wären besser

Gefährlich wird es für die Netzwerksicherheit dann, wenn im Schadensfall keine Rückschlüsse auf die Quelle einer Korrumpierung gezogen werden können. Eine gründliche Dokumentation aller Dritten, die auf das Netzwerk zugreifen, ist dafür die Voraussetzung. Die haben immerhin 56 % der Befragten. Oder sollte es eher heißen, nur 56 %? Die Gründe für keine oder mangelhafte Dokumentation kommen ITlern durchaus bekannt vor: fehlende Ressourcen, also Zeit und Personal, für die Überwachung von externen Zugriffen (45 %) und eine fehlende zentrale Kontrolle über die Beziehungen zu Dritten (37 %).

Wirken VPAM-Lösungen? - Compliance-Regeln zu komplex

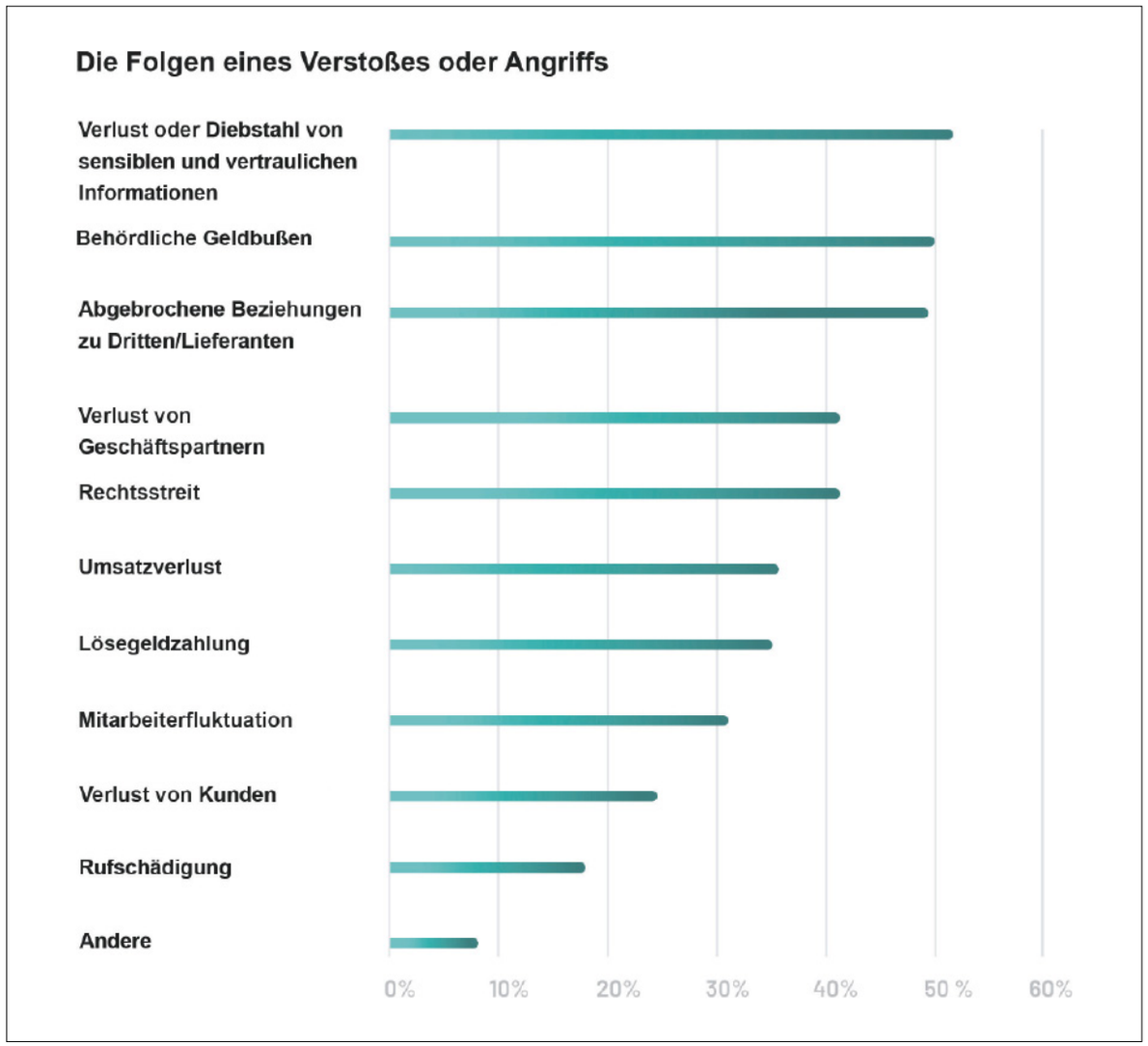
Die gute Nachricht: 77 % der Befragten bejahten, dass ihre Organisation über eine Vendor-Privileged-Access-Management-Lösung (VPAM) verfügt. Mit einer VPAM-Lösung lässt sich regeln, wie der Zugriff Externer erfolgen darf und welche Rechte er oder sie im Netzwerk hat. Allerdings sind nur 52 % dieser Gruppe davon überzeugt, dass ihre VPAM-Lösung den Missbrauch von privilegierten Zugängen wirksam verhindert. Warum?

Die Ursachen, dass trotz VPAM-Lösungen und gutem Willen in Organisationen die Zugriffe durch Externe nicht ausreichend verwaltet und überwacht werden, liegen darin, dass sich IT-Abteilungen damit überfordert fühlen und die Ressourcen zusätzlich belastet werden, sagten 38 % der Befragten. Interessant sind auch hier die genannten Gründe, denn sie bieten einen Ansatz für Verbesserungen: Die größten Hindernisse bei der Verringerung der Risiken durch Externe liegen in der fehlenden Kontrolle oder Steuerung (47 %), der Komplexität der Compliance- und gesetzlichen Anforderungen (59 %) und den unzureichenden Ressourcen oder Budgets (27 %).

Die Lösung liegt im Zero-Trust-Konzept

Vieles läuft bereits richtig, vieles liegt noch im Argen. Das Fazit aus der Studie lautet, dass Tools strategisch und konsequent angewandt werden müssen – für alle privilegierten Zugriffsanforderungen. Das Access-Management muss für interne und externe Nutzer transparent, dokumentiert und effektiv geregelt werden. Dazu dienen rollenbasierte Zugangskonzepte, Zero-Trust-Strategien mit lückenlosem Zugriffsmanagement und Multifaktor-Authentifizierung. ■

| www.imprivata.com |

Über die Studie

Das Ponemon Institut befragte Ende 2024 1.942 IT- und IT- Sicherheitsverantwortliche in den USA (733), Großbritannien (398), Deutschland (573) und Australien (238), die mit der Verwaltung von privilegierten Zugängen sowohl von Dritten als auch von internen Benutzern in ihren Organisationen vertraut sind. Die Befragten gehören Organisationen und Unternehmen aus folgenden Branchen an: Gesundheitswesen (11 %), der öffentliche Sektor (23 %), Industrie und Fertigung (32 %) sowie Finanzdienstleistungen (34 %).