SIMPLYIT LANWORKS

WIR MACHEN EXPERTENWISSEN WIRKSAM

www.lanworks.de

Catch me if you can –

Wie schützen Sie Ihr Unternehmen?

Erinnern Sie sich noch an „Catch me if you can“? Wenn Sie den Film gesehen haben, wissen Sie ja schon ziemlich genau, wie und wann Identitätsdiebstahl am besten funktioniert. Ende der 60er Jahre schlüpfte Frank Abagnale Jr. in zahlreiche Rollen, indem er glaubwürdig vorgab, jemand anderes zu sein (mal Pilot, mal Arzt oder Rechtsanwalt) als er tatsächlich war. Mit vorgetäuschter Identität hat er Menschen dazu gebracht, ihm Informationen zu geben, die er für seine Betrügereien benötigte. Keine Frage, der Begriff des Identitätsdiebstahls hat sich seither drastisch verändert. Nutzte Frank Abagnale Jr. für seine Betrügereien noch aufwendige und schwierige Methoden und Techniken (Urkunden- und Passfälschung), so genügt heute schon der Klick auf einen Link in einer Pishing-E-Mail. Oder die unbedarfte Weitergabe von Passwörtern und Nutzernamen, die es einem Betrüger heute ermöglichen, nahezu unerkannt jede beliebige Identität anzunehmen.

Identitätsdiebstahl als wesentlicher Treiber für Cyber-Kriminalität

Identitätsdiebstahl ist heute oft der Ausgangspunkt für schwerwiegende Sicherheitsverletzungen in Unternehmen. Der „Verizon Business 2020 Data Breach Investigations Report“ (DBIR 2020) berichtet, dass bei rund zwei Dritteln der insgesamt 32.000 untersuchten Sicherheitsvorfällen entweder gestohlene Anmeldeinformationen oder der „menschliche Faktor“ eine Rolle spielten.

Deutlich stärker unter Beschuss geraten sind laut DBIR 2020 auch Web- und Cloud-Applikationen: die Zahl der Angriffe hat sich nahezu verdoppelt. In über 80 Prozent dieser Fälle benutzten die Angreifer dabei gestohlene Zugangsdaten.

Ein aus unserer Sicht beunruhigender Trend. Geschäftskritische Workflows werden nicht zuletzt auch durch die seit Corona stark gestiegene Zahl an Remote-Arbeitsplätzen immer mehr in die Cloud verlagert. Eine durchgängige Sicherheit von der Cloud bis zum Endpoint der Mitarbeiter wird also immer wichtiger – und zwar für Unternehmen jeglicher Größe.

Der Mittelstand zunehmend im Visier

Sowohl der DBIR 2020 Report als auch eine aktuelle Bitkom Studie der zu Spionage und Datendiebsstahl zeigen, dass heute auch kleine und mittlere Unternehmen ein bevorzugtes Ziel für Cyber-Angriffe sind. Gerade kleinere Unternehmen sind besonders innovativ und stark in die Lieferketten von großen Konzernen eingebunden. Angreifer haben es auf Spezialwissen abgesehen oder nutzen kleinere Unternehmen als Einfallstor. So wundert es nicht, dass 88 Prozent der mittelständischen Unternehmen bereits in den Jahren 2017 und 2018 von Cyberangriffen betroffen waren. Es ist davon auszugehen, dass der Anteil betroffener Unternehmen im Jahr 2020 nochmals gestiegen ist. Doch nicht nur der Umfang und die Qualität der Angriffe haben zugenommen. Auch die finanziellen Schäden liegen laut der Studie bei über 100 Milliarden Euro pro Jahr, verursacht durch Produktionsausfälle oder Erpressung.

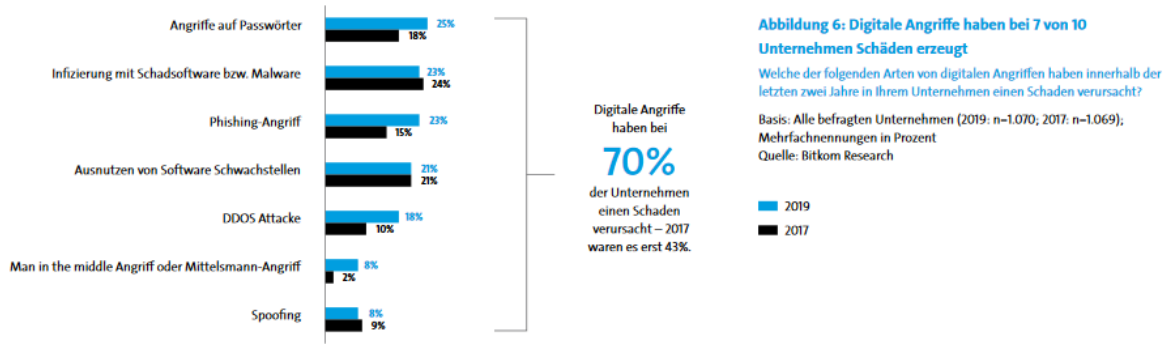

Abbildung 1 Quelle Bitkom, Studie Wirtschaftsschutz 2020, https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

Chaotische Berechtigungsstrukturen laden zum Datenklau ein

Aber nicht nur der Diebstahl digitaler Identitäten ist ein Problem. Auch mangelnde Kontrolle und Transparenz über vergebene Zugriffsrechte erhöhen die Angriffsfläche für Missbrauch. Ohne eine zentrales Rechtemanagement fehlt den IT-Verantwortlichen häufig die Kontrolle darüber, wer auf welche Benutzerkonten zugreifen kann. Wenn dann auch auf organisatorischer Ebene noch nicht geklärt ist, wer wofür autorisiert ist oder welche Unternehmensdaten als besonders kritisch einzustufen sind, sind Benutzer-Accounts häufig mit weitaus mehr Rechten ausgestattet, als für die entsprechende Rolle überhaupt notwendig wäre. Wechselt ein Mitarbeiter dann intern seine Position, wird oft übersehen, Zugriffsrechte zu löschen oder entsprechend den neuen Anforderungen anzupassen. Das führt zu oft einem Wildwuchs.

Zentrale Rechtevergabe, regelmäßige Kontrollen und Zero Trust

Ein Identity Management ermöglicht die kontrollierte Vergabe und zentrale Steuerung von Zugriffsrechten und beugt somit der Entwendung sensibler Daten vor. Eine richtlinienbasierte Rechtevergabe bietet einen guten Überblick über alle Berechtigungen und einen sicheren Rechteentzug. So lässt sich bei einem Mitarbeiterwechsel eine automatische Deprovisionierung anstoßen. Alle bisherigen Zugriffsrechte werden automatisch gesperrt. Neue Berechtigungen werden nur in dem Maß erteilt, wie sie für die neue Aufgabe benötigt werden. Das Ergebnis: Unternehmen können sensible Daten sehr früh schützen. Ein Berechtigungsaudit gibt jederzeit Aufschluss darüber, wer Zugriff auf welche Daten und Anwendungen hat. Ein Rechte-Wildwuchs ist somit kaum möglich. Die Dokumentation wird nachvollziehbar und garantiert auch die Einhaltung von Compliance-Vorgaben.

Doch damit nicht genug. Wie bereits in unserem letzten Blogbeitrag „Cyber-Resilienz – Buzzword oder Booster für mehr Sicherheit in Unternehmen“ erläutert, lässt sich das Risiko eines Angriffs nie vollständig ausschließen. Hier hilft Zero Trust mit einer mehrstufigen Authentifizierung und einem Access Management Tool - „Nie vertrauen, immer verifizieren“.

Fazit

Mit zunehmender Digitalisierung steigen auch die Angriffe. Folglich wird die Sicherheit in der IT in Zukunft über den geschäftlichen Erfolg entscheiden. Die Technologie hilft, Prozesse zu automatisieren. Sie kann aber nicht alle Probleme lösen. Nur mit der Implementierung entsprechender Regeln und Richtlinien kann das gewünschte Endergebnis erzielt werden.

Die Lanworks AG unterstützt den Aufbau, Neuaufbau und die Weiterentwicklung Ihrer Identity Management Lösung mit Expertenwissen, kompetenter Beratung und praxisorientierten Weiterbildungen.