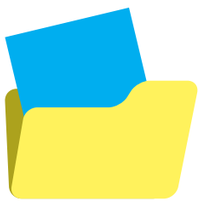
Gefahr aus dem Netz – Was tun gegen Internetkriminalität?

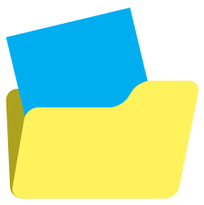
Direkte, digitale Interaktionen mit Geschäftspartnern und Cloud-Dienstleistern erhöht die Gefahr, via Internet attackiert zu werden. Doch wo die Sicherheitshebel ansetzen? Von Hadi Stiel



RISIKOKOMPETENZ

Nach Christian Ehlen, Senior Consultant bei Twinsec, ist in mittelständischen Unternehmen Risikokompetenz vorhanden. „Was hier fehlt, ist das Vermögen, Angriffen gezielt entgegenzuwirken oder diese nach kurzer Zeit zu erkennen und zu kontrollieren." Die Folge sei eine Asymmetrie zwischen denjenigen, die mit einer Sicherheitsarchitektur das Unternehmen schützen, und denen, die über die Ausnutzung weniger Schwachstellen diese Architektur zu Fall bringen können. Dies mit zusehends intelligenteren und in ihrer Auswirkung breiter ausgelegten Angriffsformen: Ihr Spektrum reicht von Ransomware über verteilte Denial-of-Service-Attacken bis hin zu maßgeschneiderten Operationen. Für die Angreifer ist die Einstiegshürde in letzter Zeit drastisch gesunken. Finanzielle Transaktionen und Smart Contracts über Technologien wie Ethereum, Bitcoin und Tor werden dazu genutzt, anonym Geld zu erpressen. Zusätzlich tragen diese Mittel dazu bei, ein Ökosystem zu errichten, innerhalb dessen verschiedene Parteien bei Angriffen kooperieren und profitieren: von der Abwicklung des Zahlungsverkehrs bis hin zur Vermietung von Angriffswerkzeugen gegen Erfolgsprämie.

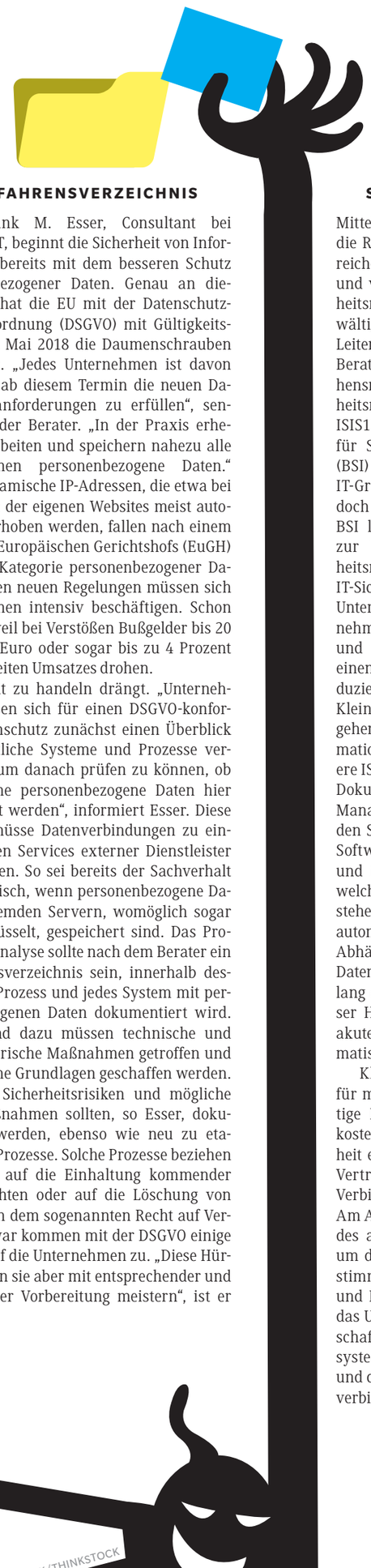
Nach dem Bericht MTrends EMEA von Fire Eye Mandiant dauert es im Schnitt 106 Tage, bis ein digitaler Einbruch erkannt wird, wobei in vielen Fällen diese Erkenntnis aufgrund von Medienveröffentlichungen oder durch Mitteilungen von Strafverfolgungsbehörden zustande kommt. Ehlen hebt aber auch positive Entwicklungen heraus, so in den Bereichen des maschinellen Lernens, der Verhaltensanalyse, der statischen und dynamischen Softwareanalyse sowie der Security Intelligence. Technologien allein reichten aber nicht aus. „Es sind Prozesse und Spezialisten notwendig, um Vorfälle zu erkennen und angemessen darauf zu reagieren", so Ehlen weiter. Deshalb sollten insbesondere mittelständische Unternehmen genau abwägen, ob sie alle Aspekte der Cyber- und Informationssicherheit eigenverantwortlich abdecken könnten. Nach mehreren Umfragen wächst in Deutschland die Akzeptanz, stattdessen auf externe Managed Security Services zurückzugreifen.



ZUGRIFFSKONTROLLE

Dem Management von Identitäten und Berechtigungen wird für den Schutz sensibler Daten, Anwendungen und Systeme eine Schlüsselrolle zukommen. „Die Problemstellung besteht dabei für die Unternehmen darin, dass sämtliche Identitäten über den kompletten Aktionsradius einschließlich der Geschäftspartner, Cloud-Dienstleister und Kunden eindeutig sind", schildert Andreas Martin, Vorstand und CEO des Consulting-Unternehmens First Attribute AG. Nur unter dieser Voraussetzung greife der zweite Schritt, die Zugriffskontrolle, umfassend und verlässlich. Je verlässlicher eindeutige Identitäten und ihre Berechtigungen ineinanderwirken, umso besser lassen sich die Identitäten schützen. Den Angreifern von innen und außen bleibt somit weniger Raum, durch Identitätslöcher zu schlüpfen und sich Berechtigungen legitimer Nutzer anzueignen.

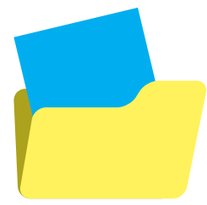
Was die Verlässlichkeit, Übersichtlichkeit und den Komfort betrifft, gibt es nach Einschätzung des Experten Nachholbedarf. „Die Nutzer müssen via Self-Service-Portal im Mittelpunkt des Identitäten- und Berechtigungsmanagements stehen." Dadurch könnten sie für sich selbst viele Verwaltungsarbeiten übernehmen, die zuvor ausschließlich Administratoren vorbehalten waren. Dies stärke über den kompletten Aktionsradius des Unternehmens nicht nur den Zugriffsschutz, sondern motiviere auch die Nutzer, in puncto Sicherheit von Daten, Anwendungen und Systemen selbst tätig zu werden. Ein solcher Nutzer-Self-Service ist schon deshalb zeitgemäß, da IT-Infrastrukturen und Anwendungsarchitekturen immer komplexer werden und teils außerhalb des Unternehmens angesiedelt sind. Hinsichtlich bei Cloud-Dienstleistern angesiedelter IT-Infrastrukturen und Anwendungsarchitekturen mit abgesetzten Verzeichnisinstanzen hat Martin klare Vorstellungen: „Die Verwaltungshoheit für die Berechtigungen auf diese externen Ressourcen sollte unbedingt im federführenden Unternehmen verbleiben." Zumal das Unternehmen generell sowohl für IT-Sicherheit als auch IT-Compliance in der gesetzlichen Haftung stehe. Martin sieht das Identitäten- und Berechtigungsmanagement schon auf dem nächsten Entwicklungssprung: „Künstliche Intelligenz wird darin Einzug halten. KI wird so für die Nutzer den Bedienungskomfort und für das Unternehmen das Niveau der umfassenden Zugriffskontrolle weiter erhöhen."



VERFAHRENSVERZEICHNIS

Nach Frank M. Esser, Consultant bei Bridging IT, beginnt die Sicherheit von Informationen bereits mit dem besseren Schutz personenbezogener Daten. Genau an dieser Stelle hat die EU mit der Datenschutz-Grundverordnung (DSGVO) mit Gültigkeitsdatum 25. Mai 2018 die Daumenschrauben angezogen. „Jedes Unternehmen ist davon betroffen, ab diesem Termin die neuen Datenschutzanforderungen zu erfüllen", sensibilisiert der Berater. „In der Praxis erheben, verarbeiten und speichern nahezu alle Unternehmen personenbezogene Daten." Selbst dynamische IP-Adressen, die etwa bei Besuchern der eigenen Websites meist automatisch erhoben werden, fallen nach einem Urteil des Europäischen Gerichtshofs (EuGH) unter die Kategorie personenbezogener Daten. Mit den neuen Regelungen müssen sich Unternehmen intensiv beschäftigen. Schon deshalb, weil bei Verstößen Bußgelder bis 20 Millionen Euro oder sogar bis zu 4 Prozent des weltweiten Umsatzes drohen.

Die Zeit zu handeln drängt. „Unternehmen müssen sich für einen DSGVO-konformen Datenschutz zunächst einen Überblick über sämtliche Systeme und Prozesse verschaffen, um danach prüfen zu können, ob und welche personenbezogene Daten hier verarbeitet werden", informiert Esser. Diese Analyse müsse Datenverbindungen zu eingebundenen Services externer Dienstleister einschließen. So sei bereits der Sachverhalt problematisch, wenn personenbezogene Daten auf fremden Servern, womöglich sogar unverschlüsselt, gespeichert sind. Das Produkt der Analyse sollte nach dem Berater ein Verfahrensverzeichnis sein, innerhalb dessen jeder Prozess und jedes System mit personenbezogenen Daten dokumentiert wird. Flankierend dazu müssen technische und organisatorische Maßnahmen getroffen und vertragliche Grundlagen geschaffen werden. Auch die Sicherheitsrisiken und mögliche Gegenmaßnahmen sollten, so Esser, dokumentiert werden, ebenso wie neu zu etablierende Prozesse. Solche Prozesse beziehen sich etwa auf die Einhaltung kommender Meldepflichten oder auf die Löschung von Daten nach dem sogenannten Recht auf Vergessen. Zwar kommen mit der DSGVO einige Hürden auf die Unternehmen zu. „Diese Hürden können sie aber mit entsprechender und rechtzeitiger Vorbereitung meistern", ist er überzeugt.



SICHERHEITSMANAGEMENT

Mittelständler können intern oft nicht auf die Ressourcen zurückgreifen, um sich hinreichend vor Angriffen aus dem Cyberspace und von innen zu schützen. Um die sicherheitsrelevanten Aufgaben dennoch zu bewältigen, empfiehlt Philipp Kleinmanns, Leiter des Geschäftsbereichs IT Factory beim Beratungshaus Materna, über das Vorgehensmodell ISIS12 ein Informationssicherheitsmanagementsystem herauszubilden. ISIS12 basiert auf dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Standardverfahren für IT-Grundschutz, ist in der Umsetzung jedoch weniger komplex als dieser. Nach dem BSI leistet ISIS12 einen wichtigen Beitrag zur Verbreitung von Informationssicherheitsmanagementsystemen sowie für mehr IT-Sicherheit in kleinen und mittelgroßen Unternehmen. „ISIS12 betrachtet die unternehmenskritischen Anwendungen, Daten und verbundenen IT-Systeme und wendet einen gegenüber dem IT-Grundschutz reduzierten Maßnahmenkatalog an", erklärt Kleinmanns die ressourcenschonendere Vorgehensweise, im Unternehmen mehr Informationssicherheit zu etablieren. Dafür steuere ISIS12 klar formulierte Anweisungen zur Dokumentation der IT sowie zum IT-Service-Management bei. Die Projektteilnehmer werden Schritt für Schritt mittels Open-Source-Software durch das ISIS12-Vorhaben geleitet und in jeder Etappe darüber unterrichtet, welche sicherheitsrelevanten Aufgaben anstehen. Installierte Hard- und Software wird automatisch erkannt und registriert, ebenso Abhängigkeiten zwischen Anwendungen, Daten und verbundenen IT-Systemen entlang digitaler Transaktionen. Aufgrund dieser Hintergrundautomatismen wird zudem akute Sicherheitsbedarf gezielt und teilautomatisiert ermittelt.

Kleinmanns ist überzeugt: „ISIS12 ist für mittelständische Unternehmen die richtige Konzeption, um schnell, einfach und kostengünstig in mehr Informationssicherheit einzusteigen, auf diese Weise für mehr Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit der Daten Sorge zu tragen." Am Anfang des Projekts steht die Ermittlung des aktuellen Reifegrads der Organisation, um das Maß an notwendiger Sicherheit bestimmen zu können. Nach der Einführung und Revision des ISIS12-Projekts kann sich das Unternehmen von der Deutschen Gesellschaft zur Zertifizierung von Managementsystemen (DQS) nach ISIS12 zertifizieren und dadurch das erreichte Sicherheitsniveau verbindlich bestätigen lassen.

ANALYSESTRUKTUR

Harald Reisinger, Geschäftsführer und Mitbegründer der österreichischen IT-Sicherheitsfirma Radar Services, spricht angesichts der wachsenden Bedrohungslage, in der mittelständische Unternehmen schweben, von Naivität im Umgang mit IT-Sicherheit. „Selbst wenn Sicherheitslücken aufgrund von Schwachstellen in der Software seit Wochen über Medien bekannt sind, werden sie oftmals nicht über sogenannte Patches geschlossen", stellt er ernüchtert fest. Er fordert die Unternehmen auf, eine saubere Analysestruktur zu implementieren, um Schwachstellen in Programmen sowie abnormen Verhaltensweisen in IT-Systemen und verdächtigen Datenströmen auf Verbindungen auf die Spur zu kommen. Er plädiert in diesem Zusammenhang für den Einsatz von IT Security Monitoring als Frühwarnsystem. „IT Security Monitoring sammelt Ereignisdaten, analysiert sie und kristallisiert diejenigen heraus, die auf einen Missbrauch der IT und von Anwendungen, auf Betrug oder auf andere Sicherheitsbedrohungen hinweisen." Für Reisinger steht außer Frage: „Nur durch die Kombination von automatisierten Erkennungsmethoden und anschließender expertengestützter Detailanalyse kann im Unternehmen ein tagesaktuelles Risikolagebild für gezielte und schnelle Gegenmaßnahmen entwickelt werden."

Dafür sollte IT Security Monitoring in voller Breite überwachen und analysieren: an sämtlichen Anwendungen und IT-Systemen, an allen internen Verbindungen sowie an sämtlichen Zugängen zum Internet. Eine IT-Security-Monitoring-Lösung der neuen Generation muss zudem komplexe Muster von Cyber-Angriffen sowie Advanced Cyber Attacks mit Hilfe verhaltensbasierender Analysemethoden durch Anwendung statistischer Modelle, rekursiver Verfahren und selbstlernender Algorithmen erkennen. IT Security Monitoring sieht der Geschäftsführer in Dienstleisterhänden besser aufgehoben. Dafür sprechen nach seiner Einschätzung sowohl Kostengründe als auch der Mangel an Sicherheitsspezialisten in den Unternehmen, was im Eigenbetrieb zudem auf Kosten der Detailanalyse gehen würde, um von den Risikohinweisen auf die notwendigen Gegenmaßnahmen zu schließen.

FOTO JESADAPHORN/ISTOCK/THINKSTOCK