von René Kerkhoff, Analyst für die Sektoren Technologie, Automotive und Retail bei der DJE Kapital AG und Fondsmanager des DJE – Mittelstand & Innovation

Cyber Security im Fokus der Anleger

Pullach im Isartal, 22. Mai 2019 – Der digitale Wandel hat längst nahezu alle Lebensbereiche und damit sämtliche Branchen und Sektoren erfasst. Durch die digitale Transformation werden zahlreiche Prozesse vereinfacht und die Produktivität gesteigert. Eine Studie der Roland Berger Strategy Consultants im Auftrag des Bundesverbands der Deutschen Industrie rechnet bis 2025 mit einer zusätzlichen Wertschöpfung in Europa von bis zu 1,25 Billionen Euro. Allerdings erhöht die Digitalisierung auch die Anfälligkeit der Unternehmen für Cyber-Attacken.

Laut Bundesministerium für Sicherheit in der Informationstechnik (BSI) wurden in den Jahren 2016 und 2017 rund 70 Prozent aller Unternehmen in Deutschland über das Internet angegriffen. Die Hälfte dieser Angriffe war erfolgreich, wiederum knapp die Hälfte der erfolgreichen Angriffe führte zu Produktions- und Betriebsausfällen. Die Gesamtkosten für Schäden aus Cyber-Angriffen belief sich in diesem Zeitraum auf über 43 Milliarden Euro, unter anderem für die Wiederherstellung der Systeme und die Kosten für die Aufklärung der Angriffe. Der größte Teil der Angriffe erfolgte über Malware, also infizierte Software, gefolgt von Hacking-Angriffen und Angriffen auf die Netzwerkinfrastrukturen der Unternehmen.

Steigende Nachfrage nach digitalen Cyber Security-Lösungen

Konzentrierten sich bisher die Angriffe hauptsächlich auf Browser, Betriebssysteme und JavaScript, bieten digitalisierte Unternehmen heute mehr Angriffsmöglichkeiten. Zum Beispiel werden E-Mail-Verschlüsselungen, Smart Cards, Prozessoren/Chips und Überwachungskameras Ziel von Cyber-Attacken. Zudem tauchen pro Tag 390.000 neue Schadprogramm-Varianten auf, die das Angriffsrisiko für Unternehmen zusätzlich erhöhen. Immer mehr Unternehmen, insbesondere Großkonzerne, sehen diese

Entwicklung für ihre Betriebsfähigkeit als kritisch an und investieren daher vermehrt in den Schutz ihrer IT-Infrastruktur.

Laut dem deutschen Digitalverband Bitkom gaben Unternehmen im Jahr 2018 rund vier Milliarden Euro für ihre IT-Sicherheit aus (9 Prozent mehr als im Vorjahr). Dazu zählen Ausgaben für die laufende Überwachung der Netzwerke, für regelmäßige Überprüfung der Zugriffsberechtigungen und Schwachstellenanalyse sowie für die Beratung durch externe Spezialisten. Mussten Unternehmen früher in analogen Werkschutz investieren, um ihr Warenlager zu schützen, müssen sie heute digitale Sicherheitssysteme ausbauen. Die Nachfrage an Cyber Security-Lösungen wird dementsprechend mindestens so stark steigen wie die Digitalisierungsrate in Unternehmen, damit diese ihr geistiges Eigentum schützen können.

Cyber Security als Dienstleistung

Rund 55 Prozent der Ausgaben für IT-Sicherheit investierten die Unternehmen 2018 in Dienstleistungen für digitale Sicherheit, unter anderem für die Beratung durch IT-Security Consultants oder für Outsourcing der IT-Security Dienste an Managed Security Services Providers (MSSP). IT-Service Consultants helfen Unternehmen dabei, die eigene Sicherheitsstrategie zu überprüfen und notwendige Veränderungen zu implementieren. Dazu gehören Risiko- und Schwachstellenanalysen, Notfall-Support oder Compliance-Richtlinien und gesetzliche Anforderungen.

MSSPs sind auf Cybersicherheit spezialisierte IT-Dienstleister, deren Geschäftsmodell Cybersecurity-as-a-Service ist. Das bedeutet: Sie übernehmen die Überwachung und Verwaltung von Sicherheitsgeräten und -systemen für den Auftraggeber und kümmern sich um Systemupdates und -upgrades. Der Auftraggeber kann durch das Outsourcing Kosten einsparen und gleichzeitig die Sicherheit erhöhen. Aufgrund der weiter steigenden Anforderungen an Cyber-Abwehrstrategien werden Unternehmen auch in Zukunft diese komplexen und zeitintensiven Vorgänge auslagern.

MARKTKOMMENTAR

Intelligente Sicherheitssoftware auf dem Vormarsch

Die zunehmende Digitalisierung und dadurch steigende Vernetzung der Wirtschaft verändert die Anforderungen an die Security-Software von Unternehmen. Wurden früher hauptsächlich Virenscanner und standardisierte Firewalls zur Abwehr von Schadsoftware verwendet, sind im Zeitalter des cloudbasierten Arbeitens intelligente Lösungen notwendig, die mehr als nur den einzelnen PC oder Laptop sichern. Viele Softwareunternehmen bieten ihre aktuelle Cyber Security-Software als Abonnementlösung (Software-as-a-Service) an und sichern Clouds und Rechenzentren. Diese Unternehmen entwickeln Softwarelösungen, die mit Hilfe von Machine Learning intelligent und selbstlernend sind. So erkennen sie frühzeitig Schadsoftware, immunisieren sie und versuchen die Sicherheitslücke selbstständig zu schließen. Die Abonnenten des Software-as-a-Service Modells profitieren von der stetigen Weiterentwicklung der Systeme, da Updates automatisch installiert werden.

Darüber hinaus gibt es im Bereich Cyber Security-Software einige Spezialanbieter, die sich auf einzelne Segmente, zum Beispiel Kommunikationsnetzwerke oder kritische Technologien, fokussieren. Durch die Integration von Security-Software in Kommunikationsnetzwerken können Endkonsumenten einfach und plattformunabhängig geschützt werden. Algorithmen und künstliche Intelligenz können zuverlässig Bedrohungen erkennen und bekämpfen. Durch die Installation im Netzwerk benötigt die Software keinerlei Einblick in die Systeme der Netzanbieter, wodurch Kunden- und Transaktionsdaten geschützt sind.

Hardware-basierte Sicherheitssysteme noch unterschätzt

Weiterhin unterschätzt wird der Einsatz von Hardware zur Vermeidung von Cyber-Angriffen. Zu den Hardware-Sicherheitsmodulen (HSMs) gehören unter anderem Token, externe Geräte, Smartcards oder Module, die an andere Geräte angeschlossen werden. HSMs sind durch physische Maßnahmen (Bohrschutzfolie, Eingießen von Chips) und Sensoren (Temperatur- und Spannungssensoren) vor physikalischen, mechanischen oder chemischen Anwendungen geschützt.

Mit Hilfe von HSMs können kryptographische Operationen gesichert und ein sicherer, verschlüsselter Datenaustausch gewährleistet werden. Dabei werden unter anderem kryptografische Schlüssel erzeugt und verwaltet, sowie Signier- und Verschlüsselungsalgorithmen bereitgestellt. HSMs kommen in verschiedenen Segmenten zum Einsatz, zum Beispiel in der Industrie, wo kritische Infrastrukturen vernetzter Produktionsanlagen durch Netzwerkverschlüsselung abgesichert werden. Der Bereich Automotive nutzt HSMs beispielsweise im Smart Connected Car und das Gesundheitswesen benötigt die Technik für die Telematikinfrastruktur.

Cyber Security bietet attraktive Anlagechancen

Es gibt also verschiedene Wege geistiges Eigentum von Firmen zu schützen. Cyber Security ist zwar bereits jetzt ein wichtiges Thema, jedoch wird es aufgrund der stärkeren Digitalisierung in Zukunft noch bedeutender. Vor allem für Small- und Mid-Cap-Investoren bieten Unternehmen aus diesem Bereich interessante Anlagemöglichkeiten. Auch der DJE – Mittelstand & Innovation nutzt diese Entwicklungen. Wir fokussieren uns dabei auf die sogenannten Hidden Champions, die mit Innovationskraft, starken Wachstumsraten und hohen Marktanteilen in strukturell wachsenden Märkten überzeugen. Wir legen dabei großen Wert auf Unternehmensbesuche, um Chancen und Risiken gemeinsam mit der Unternehmensführung zu analysieren und einen tiefen Einblick in die Geschäftstätigkeiten des Unternehmens zu bekommen.

Über die Dr. Jens Ehrhardt Gruppe

Die DJE Kapital AG ist seit 45 Jahren als unabhängige Vermögensverwaltung am Kapitalmarkt aktiv. Das Unternehmen aus Pullach bei München verwaltet mit über 135 Mitarbeitern (davon rund 25 Fondsmanager und Analysten) aktuell über 12,6 Milliarden Euro (Stand: 31.03.2019) in den Bereichen individuelle Vermögensverwaltung, institutionelles Asset Management sowie Publikumsfonds. Zudem bietet die DJE Kapital AG seit 2017 mit Solidvest eine einzeltitelbasierte Online-Vermögensverwaltung an – als digitale Lösung im Rahmen aktiv gemanagter Depots. Das Online-Konzept basiert auf den breiten Kompetenzen in Vermögensverwaltung und Anlagestrategie der DJE Kapital AG – und ermöglicht ein diversifiziertes Portfolio nach individuellem Rendite-Risiko-Profil mit persönlichen Themenschwerpunkten im Aktienbereich. Vorstandsvorsitzender ist Dr.

Jens Ehrhardt, sein Stellvertreter Dr. Jan Ehrhardt. Kern des Anlageprozesses und aller Investmententscheidungen ist die FMM-Methode (fundamental, monetär, markttechnisch), welche auf dem hauseigenen, unabhängigen Research basiert. Der Anspruch der DJE Kapital AG ist, ihren Kunden weitsichtige Kapitalmarktexpertise in allen Marktphasen zu bieten.

Unternehmenskontakt
Simone Ausfelder
+49 (0)89 790453-661
simone.ausfelder@dje.de

Pressekontakt
Instinctif Partners
Johannes Zenner // Sophie Horrion
+49 (0)69 133 896-21 // +49 (0)221 4 20 75-11
johannes.zenner@instinctif.com // sophie.horrion@instinctif.com