IDC Studie zu Cyber Security 2020+: COVID-19 lässt Budgets steigen, Sicherheitssituation bleibt bedenklich

Die IT-Sicherheitslage in Deutschland ist nach wie vor angespannt. Die wachsende Komplexität der IT-Landschaften, die Agilität und Masse der Cyber-Attacken sowie die steigenden Compliance-Anforderungen lassen sich mit den implementierten, aber offenbar unzulänglichen IT-Security-Ressourcen immer schwerer beherrschen. COVID-19 und die damit verbundene Abwanderung zahlloser Mitarbeiter in die Home-Offices war und ist ein weiterer Prüfstein für die Qualität der Abwehr- und Reaktionsfähigkeit der Unternehmen auf industrieübergreifende Ereignisse von globaler Reichweite. Umfassende IT-Security wird kritischer für den wirtschaftlichen Erfolg jedes Unternehmens und jeder Organisation.

Eine neue IDC Studie zeigt auf, wo die Unternehmen nachschärfen müssen und welche Pläne sie haben:

- 78 Prozent der befragten Unternehmen in Deutschland wurden erfolgreich attackiert
- 63 Prozent betonen, dass Cyber-Risiken eine veränderte Security-Architektur erfordern
- Netzwerk-Security, Data Protection und Cloud Security sind die Top-Themen bei IT- Security

IDC hat im August 2020 in Deutschland IT- und Fachentscheider aus 210 Organisationen mit mehr als 100 Mitarbeitern befragt und detaillierte Einblicke in die Umsetzungspläne, Herausforderungen und Erfolgsfaktoren bei Cyber Security erhalten.

Fast jedes Unternehmen ist von Attacken betroffen, die Reaktionen darauf sind deutlich zu schwach

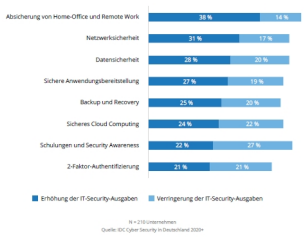
Lösungen für IT-Sicherheit existieren in allen Unternehmen. Vorranging in kleinen und mittleren Unternehmen

vertrauen aber noch deutlich zu viele Verantwortliche auf „Bordlösungen“ und Standardeinstellungen. Das ist hochriskant. 78 Prozent der befragten Unternehmen wurden bereits mit Sicherheitsvorfällen konfrontiert. „Das Ziel von Angriffen ist immer ein wirtschaftlicher Schaden in den Zielunternehmen, wie finanzielle Einbußen, Verlust von geistigem Eigentum, Rufschädigung oder Kundenverlust. Wenn die IT ruht und die Daten nicht verfügbar sind, dann hat das direkte finanzielle Auswirkungen“, erläutert Matthias Zacher, Senior Consulting Manager und Projektleiter. 64 Prozent der Befragten betonen, dass Advanced-Security-Lösungen und Next Gen Security (z. B. analytische und eventbasierte, proaktive Lösungen) wichtige Ansätze zur Verbesserung der IT-Sicherheit sind. Zwar sind in vielen Firmen neben den klassischen Security- Tools auch Cyber-Security-Lösungen vorhanden, doch die Durchdringungsrate ist noch viel zu gering. Allerdings besteht nach wie vor umfassender Erläuterungsbedarf in vielen Unternehmen darüber, wie sie moderne Lösungen beim Aufspüren und Bekämpfen von Advanced Threats unterstützen können.

Abbildung 1: Wie haben sich aufgrund von COVID-19 die IT-Security-Ausgaben Ihres

Unternehmens in folgenden Bereichen geändert?

Figure 1



COVID-19: Security-Budgets steigen – allerdings nicht in allen Unternehmen

COVID-19 stellt nach wie vor für alle Unternehmen einen großen Unsicherheitsfaktor dar. Das gilt weniger für die geschäftliche Entwicklung der vergangenen Monate, sondern vielmehr für die kommenden Wochen und Monate. IT-Security zählt zu den „Gewinnern“ der aktuellen Situation.

Für die Absicherung von Home-Office und Remote Work haben 38 Prozent der Befragten ihre Budgets erhöht. Hierzu zählen Ausgaben für die bessere Absicherung der Endgeräte und Investitionen für Data Protection. 31 Prozent der Befragten wollen mehr für Netzwerksicherheit ausgeben. Dringliche Investitionen in Backup und Recovery, sicheres Cloud Computing oder stärkeres Identity und Access Management stehen weiterhin aus und müssen aus IDC Sicht kurzfristig adressiert werden.

Längst überfällig: Netzwerk-Security rückt stärker in den Fokus

Mit einer Nennung von 37 Prozent führt Netzwerk-Security die Liste der wichtigsten Themen für das Jahr 2020 an. Aus Sicht von IDC war es längst überfällig, dass das Netzwerk und seine Absicherung stärker in den Blickwinkel der IT-Entscheider rücken. COVID-19, Remote Work, die effiziente und kostengünstige Anbindung von Niederlassungen mit SD-WAN sowie weitere neue Technologien weisen dem Netzwerk eine tragende Rolle in Informations- und Telekommunikationstechnologie zu und fordern ein umfassendes Update der Netzwerk-Security und der Security-Architektur in den Unternehmen.

Wichtige Themen 2021: Cloud Security und Digital Trust

Die Cloud einwickelt sich immer stärker zum integralen Bestandteil der IT-Landschaft. Aus diesem Grund müssen sich Unternehmen deutlich stärker als bisher auf Cloud Security konzentrieren.

Mit hybriden Clouds und Multi Clouds steigen sowohl die Zahl der potenziellen Angriffspunkte als auch die Anzahl der Personen und Identitäten, die gemeinsam an einer Aufgabe arbeiten oder in einem Ökosystem miteinander agieren. Das erfordert eine hohe Robustheit der Lösungen, um potenziellen Angreifern

wenig Raum zu lassen bzw. sofort reagieren zu können. Rund 70 Prozent der Befragten betonen, dass hybride Clouds und Multi Clouds eine angepasste Security-Architektur erfordern, um Angriffsmöglichkeiten bereits im Vorfeld zu reduzieren. Ein weiterer Aspekt zur Stärkung der Cyber Security und Cloud Security im Besonderen ist Vertrauen bzw. Digital Trust. Mit Digital Trust sichern Unternehmen ihren Geschäftspartnern und der Öffentlichkeit zu, dass sie auf verschiedenen Stufen umfassende Maßnahmen durchgeführt haben, um als vertrauenswürdiger Partner in digitalen Ökosystemen akzeptiert zu werden. Aus IDC Sicht ist Digital Trust gerade in Krisenzeiten essenziell und sollte nicht vernachlässigt werden.

Die nächsten Schritte: Mehr Integration, mehr Automatisierung

Bei allen genannten Zielsetzungen und Hürden bleibt der Mangel an qualifizierten Mitarbeitern eine permanente Herausforderung. Die Integration von Security-Lösungen und Automatisierung ist ein wichtiger Baustein, um den Fachkräftemangel in Ansätzen zu kompensieren und zur Erhöhung der Sicherheit beizutragen. Die Integration von verschiedenen Security-Lösungen ist seit Jahren eine Dauerbaustelle in den Unternehmen, an der die IT-Security-Industrie aufgrund mangelnder Integrationsfähigkeit

der Lösungen ihren Anteil hat. Nun kommt aber langsam Bewegung in die Sache. 49 Prozent der Befragten nutzen derzeit Lösungen zur engeren Verzahnung der Komponenten eines Anbieters. Jeweils 42 Prozent korrelieren Security-Lösungen mit Netzwerk-Management-Lösungen und integrierten Lösungen Dritter auf Basis eines Kommunikations-Layers. Diese Ansätze unterstreichen das Streben nach proaktivem Schutz, nach Monitoring und Transparenz als wichtige Voraussetzung für reaktionsschnelles Handeln.

Analytische Ansätze und KI-basierte Funktionalitäten bieten hier einen deutlichen Mehrwert. Wenn es den Unternehmen noch besser als bisher gelingt, IT-Sicherheit in die Planung, Initiierung und Bewertung aller neuen Business-Initiativen von Anfang an einzubinden, dann sind wichtige Hausaufgaben gemacht.

Fazit und Ausblick

IT-Sicherheit erhält nach wie vor nicht die Aufmerksamkeit, die zur erfolgreichen Absicherung der Betriebsabläufe erforderlich ist. Die aktuelle Studie zeigt – wie auch schon die letzte – deutlich, dass viele Organisationen immer noch unzureichend geschützt sind. Zwar sind ein Basisschutz und Standard-Security-Lösungen in allen Organisationen vorhanden. Das allein reicht aber immer

weniger dafür aus, der Vielzahl und der Intensität der Angriffe zu begegnen und die Ausgangslage nach erfolgreichen Attacken wiederherzustellen.

Die aktuelle Anforderung besteht für die meisten Unternehmen explizit darin, ihre IT-Security-Strategie auf den Prüfstand zu stellen, um neue Technologien und Lösungsansätze, digitales Business und neue Formen der Zusammenarbeit zwischen unterschiedlichen Marktteilnehmern umfassend abzusichern und die Agilität und Widerstandsfähigkeit ihrer Organisation gegenüber unerwarteten Vorkommnissen zu erhöhen. Integration, Automatisierung und eine kontinuierliche Optimierung von Security-Prozessen über alle IT-Domains und Business-Domains hinweg sind der Schlüssel zum Erfolg. Das muss das gemeinsame Ziel von Anbietern und Anwendern sein.

Gemessen an der aktuellen Befragung haben die meisten Unternehmen in Deutschland die Herausforderungen nach IDC Einschätzungen erkannt, müssen aber an vielen Stellschrauben drehen, um für die Herausforderungen, die da kommen, gewappnet zu sein.

IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. Additional information can be found at www.idc.com. All product and company names may be trademarks or registered trademarks of their respective holders.

For more information contact:

Matthias Zacher
mzacher@idc.com
+49 69 90502-116
Katja Schmalen
kschmalen@idc.com
+49 69 90502-115