IBM-Ponemon Studie zur Resilienz gegen Cyberangriffe: Mehr als die Hälfte der deutschen Unternehmen testen ihre Notfallpläne nicht

Automatisierung verbessert die Erkennung und Eindämmung von Cyberangriffen in Deutschland um 46 Prozent

CAMBRIDGE, MA, USA – 11. April 2019: Die Ergebnisse der vierten, jährlichen Benchmark-Studie zur Cyberresilienz, vom Ponemon Institute durchgeführt und von IBM Resilient gesponsert, ist heute veröffentlicht worden. In „The 2019 Cyber Resilient Organization“ wird untersucht, inwieweit Unternehmen in der Lage sind, trotz einer Cyberattacke ihre Geschäftsprozesse, Kernaufgaben und allgemeine Integrität aufrechtzuerhalten.

Die Ergebnisse legen offen, dass eine große Mehrheit der Unternehmen noch immer nicht darauf vorbereitet ist, angemessen auf Cyberangriffe zu reagieren. 67 Prozent der deutschen Unternehmen haben keinen einheitlichen, unternehmensweiten Notfallplan.

Obwohl Studien zeigen, dass Unternehmen durchschnittlich über eine Million US-Dollar einsparen[1], wenn sie innerhalb von 30 Tagen auf einen Cyberangriff reagieren können, sind die Defizite bei der Notfallplanung in den letzten vier Jahren konstant geblieben. Von den Unternehmen in Deutschland, die über einen Notfallplan verfügen, testen mehr als die Hälfte (56 Prozent) ihre Pläne nicht regelmäßig. Sie verpassen so die Chance, die komplexen Prozesse und notwendige Koordination innerhalb der Firma, die nach einem Angriff nötig sind, vorzubereiten und zu üben.

Die anhaltenden Schwierigkeiten bei der Umsetzung des Notfallplans wirken sich auch auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO) aus. Obwohl die DSGVO in Kürze ihr einjähriges Jubiläum feiert, geben fast die Hälfte der weltweit Befragten (46 Prozent) an, dass ihr Unternehmen die Datenschutz-Grundverordnung noch nicht vollständig einhält.

„Wenn es darum geht, auf einen Cyberangriff zu reagieren, ist fehlende Planung der erste Schritt zum Misserfolg. Die Notfallpläne müssen daher regelmäßig auf Herz und Nieren geprüft werden. Damit ein solches Programm aufrechterhalten werden kann, bedarf es der vollen Unterstützung des Vorstands, um in die notwendigen Mitarbeiter, Prozesse und Technologien zu investieren“, sagt Ted Julian, VP of Product Management und Mitgründer von IBM Resilient. „Sofern die richtige Planung mit Investitionen in die Automatisierung kombiniert wird, können Unternehmen bei einem Datenverlust Millionen Dollar sparen.“

Weitere Studienergebnisse:

[1] Quelle: IBM-Ponemon Studie zu Kosten bei Datenpannen

- **Automatisierung im Cyberschutz nimmt zu** – 30 Prozent der Befragten aus Deutschland geben an, dass ihr Unternehmen Automatisierungstechnologien wie Identitätsmanagement und Authentifizierung sowie Incident-Response-Plattformen und Sicherheitsinformations- und Ereignismanagement-Systeme (SIEM) signifikant einsetzt, um auf Cyberattacken zu reagieren.
- **Fachkräfte machen den Unterschied** – 60 Prozent der befragten Unternehmen aus Deutschland sind der Meinung, dass gutes Fachpersonal im Bereich Cybersicherheit die Widerstandsfähigkeit gegen Angriffe erhöht.
- **Datenschutz und Cybersicherheit gehen Hand in Hand** – Um ihr Unternehmen widerstandsfähiger zu machen, ist es laut 66 Prozent der deutschen Befragten von Nöten, den Stellenwert von Datenschutz und Cybersicherheit gleichzusetzen.

Automatisierung zur Cyberabwehr wird wichtiger

In der diesjährigen Studie wurde zum ersten Mal gemessen, inwiefern sich automatisierte Sicherheitstechnologien auf die Widerstandsfähigkeit auswirken. Um menschliche Eingriffe bei der Identifizierung und Eindämmung einer Datenpanne zu unterstützen oder zu ersetzen, bedarf es neben dem Einsatz von Künstlicher Intelligenz (KI), maschinellem Lernen und Analytics auch der Orchestrierung, also dem flexiblen Kombinieren mehrerer Services oder Dienste.

Nur 23 Prozent aller weltweit Befragten nutzen Automatisierung in signifikantem Umgang. Bei 77 Prozent der Unternehmen kommt Automatisierung stattdessen nur mäßig oder gar nicht zum Einsatz. Jene Unternehmen, die stark auf Automatisierung setzen, schätzen ihre Fähigkeit höher ein, Cyberangriffe zu verhindern (69 Prozent vs. 53 Prozent), einen Angriff zu erkennen (76 Prozent vs. 53 Prozent), auf diesen zu reagieren (68 Prozent vs. 53 Prozent) und eine Cyberattacke einzudämmen (74 Prozent vs. 49 Prozent).

Wer Automatisierung nicht nutzt, verpasst die Gelegenheit, die eigene Widerstandsfähigkeit gegen Cyberangriffe zu stärken – und bares Geld zu sparen: Die Cost of a Data Breach-Studie von 2018 zeigt, dass Unternehmen 1,55 Millionen Dollar bei den Gesamtkosten einer Datenpanne einsparen, wenn sie automatisierte Sicherheitstechnologien in großem Umfang eingesetzt hatten. Im Gegensatz dazu hatten Unternehmen ohne Sicherheitsautomatisierung im Falle eines Datenverstoßes wesentlich höhere Gesamtkosten.

Qualifikationslücken wirken sich immer noch auf die Widerstandsfähigkeit aus

Auch Qualifikationslücken im Bereich Cybersicherheit schwächen die Widerstandsfähigkeit gegen Angriffe, da Teams unterbesetzt und nicht in der Lage sind, Ressourcen und Bedürfnisse angemessen zu verwalten. Es fehlen Mitarbeiter, berichtet wird von zehn bis 20 offene Stellen in Cybersicherheitsteams, um die Notfallpläne in den Unternehmen ordnungsgemäß zu warten und zu testen. Nur 30 Prozent der weltweit Befragten geben an, dass das Personal ausreicht, um ein hohes Maß an Widerstandsfähigkeit zu erreichen. Auch in Deutschland wird händeringend nach Fachpersonal gesucht: 86 Prozent der Befragten bewerten das Problem, qualifiziertes Cybersicherheitspersonal einzustellen und zu halten, als mäßig hoch bis hoch.

Darüber hinaus geben 29 Prozent der Befragten aus Deutschland zu, dass ihr Unternehmen zu viele isolierte Sicherheitstools einsetzt. Das erhöht letztendlich die Komplexität des Betriebs und beeinträchtigt einen vollständigen Überblick über die gesamte Sicherheitslage.

Privatsphäre wird immer wichtiger
Die Unternehmen erkennen inzwischen, dass das Zusammenspiel von Datenschutz und Cybersicherheit die Widerstandsfähigkeit stärkt. 66 Prozent der deutschen Unternehmen geben an, dass die Ausrichtung der Teams unerlässlich für den Aufbau einer widerstandsfähigen Infrastruktur ist. Der Großteil der Befragten glaubt, dass der Datenschutz immer wichtiger wird, insbesondere seit dem Inkrafttreten neuer Vorschriften wie der DSGVO und dem California Consumer Privacy Act. Der Datenschutz spielt daher auch bei IT-Kaufentscheidungen eine wichtige Rolle.

Für 56 Prozent der weltweit Befragten ist die Gefahr des Informationsverlusts oder Diebstahls der wichtigste Faktor, um Ausgaben für die Cybersicherheit zu rechtfertigen. Auch Verbraucher fordern, dass Unternehmen mehr tun, um ihre Daten aktiv zu schützen. Laut einer aktuellen Umfrage von IBM ist es 78 Prozent der Befragten besonders wichtig, dass Unternehmen ihre Daten privat halten. Nur 20 Prozent vertrauen Organisationen, mit denen sie interagieren, wenn es um den Schutz ihrer Daten geht.

Auch die Ergebnisse der IBM Studie zur Widerstandsfähigkeit von Unternehmen unterstreicht, dass der Datenschutz in Unternehmen zu einer der obersten Prioritäten geworden ist. So beschäftigen die meisten Unternehmen einen Datenschutzbeauftragten, 73 Prozent der weltweit Befragten haben sogar einen Chief Privacy Officer.

Die globale IBM-Ponemon Umfrage liefert Erkenntnisse von mehr als 3.600 Sicherheits- und IT-Experten aus der ganzen Welt, darunter die Vereinigten Staaten, Kanada, Großbritannien, Frankreich, Deutschland, Brasilien, Australien, der Mittlere Osten und der asiatisch-pazifische Raum. Aus Deutschland wurden 384 Sicherheits- und IT-Experten befragt.

Die Zusammenfassung der Studienergebnisse kann hier heruntergeladen werden.

Vollständige Berichte & Anmeldung zum Webinar
Laden Sie die Studie „The 2019 Study on the Cyber Resilient Organization“ für die vollständigen Ergebnisse herunter.

Melden Sie sich für unser nächstes Webinar an: "Titel“, das am [Datum / Uhrzeit] stattfindet.

Über IBM Security
IBM Security bietet eines der fortschrittlichsten und integriertesten Portfolios an Produkten und Dienstleistungen für die Unternehmenssicherheit. Das Portfolio, das von der weltweit agierenden IBM X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Risiken

effektiv zu managen und sich gegen neue Bedrohungen zu schützen. IBM betreibt eine der weltweit größten Forschungs-, Entwicklungs- und Serviceorganisationen für Sicherheit, überwacht 35 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hält weltweit mehr als 8.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie IBMSecurity auf Twitter oder besuchen Sie den IBM Security Intelligence blog.