

Deutsche Unternehmen weltweit führend bei Security-Automatisierung

IBM „Cost of a Data Breach“-Studie 2020: Security-Automatisierung senkt die Kosten von Datenpannen beträchtlich

CAMBRIDGE, MA, USA, Ehningen, 29. Juli 2020: Deutschland führt weltweit in der Security-Automatisierung das zeigen die neuesten Ergebnisse der heute von IBM Security und dem Ponemon Institut veröffentlichten „Cost of a Data Breach“- Studie. In Deutschland nutzen 75 Prozent der Unternehmen Security Automatisierung, 30 Prozent davon haben Systeme für die Sicherheitsautomatisierung bereits vollständig umgesetzt. Gemessen am globalen Durchschnitt von 21 Prozent ist das der höchste Wert weltweit.

Die aktuellen Studienergebnisse von IBM Security zeigen, dass die globalen Kosten von Datenpannen erstmals leicht gesunken sind: Die durchschnittlichen Kosten pro Datenpanne lagen 2019 bei 3,86 Millionen US-Dollar, und somit 1,1 Prozent niedriger als 2018. Security-Automatisierung und die verbesserte Dateneinsicht durch die Datenschutzgrundverordnung (DSGVO) sind die größten Treiber dieser Kostensenkung.

Dennoch weisen die Ergebnisse auch auf die immer größer werdende Kluft hin, die sich zwischen Unternehmen auftut, die Security-Automatisierung nutzen und solchen, die es nicht tun: Für nicht-automatisierte Unternehmen waren Datenpannen 2019 mit sechs Millionen US-Dollar mehr als zwei Mal so teuer wie für Unternehmen, die auf Künstliche Intelligenz, Machine Learning und Orchestrierung setzen (2,45 Millionen US-Dollar).

Automatisierung ist auch bei der schnellen Reaktion auf einen Vorfall wichtig: Automatisierte Unternehmen sind 74 Tage schneller bei der Reaktion und Eindämmung eines Vorfalles als Unternehmen ohne Smart-Tech (308 Tage). Deutsche Unternehmen reagieren mit nur 160 Tagen am schnellsten auf Datenpannen, im globalen Vergleich sind es 280 Tage. Die Eindämmung eines Vorfalles dauert hierzulande insgesamt nur etwa einen Monat, und das spart Geld: Datenpannen, für deren Identifizierung und Eindämmung mehr als 200 Tage benötigt werden, sind im Durchschnitt über eine Million US Dollar teurer als Pannen, die in weniger als 200 Tagen behoben werden.

„Wenn es um die Fähigkeit von Unternehmen geht, die Auswirkungen einer Datenpanne abzufedern, sehen wir allmählich einen klaren Vorteil für Unternehmen, die in automatisierte Technologien investiert haben“, so Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence.

Eine Auswahl weiterer Studienergebnisse:

Cyberangriffe boomen in Deutschland: Mit 57 Prozent gehen die meisten Datenvorfälle hierzulande auf böswillige Angriffe zurück, das entspricht nach dem Mittleren Osten (59 Prozent) dem zweithöchsten Wert weltweit. 24 Prozent der Datenpannen in Deutschland gehen von Systemfehlern aus.

Die größten Einfallstore für Hacker: Fast 40 Prozent der Angreifer nutzten die Zugangsdaten von Mitarbeitern oder fehlerhafte Cloud-Konfigurationen aus, um ins Firmennetzwerk zu gelangen. Angreifer haben bei einem von fünf untersuchten Verstößen zuvor aufgedeckte E-Mails und Passwörter verwendet.

Home Office mit Folgen: 70 Prozent der befragten Unternehmen, die während der Covid-19-Pandemie Home-Office eingeführt haben, rechnen mit mehr Datenpannen und überdenken deswegen ihre Sicherheitsstrategie. Datenpannen

durch Remote-Mitarbeiter sind teurer, die durchschnittlichen Gesamtkosten belaufen sich auf vier Millionen US-Dollar.

Personenbezogene Kundendaten sind am teuersten: Bei 80 Prozent der Datenpannen 2019 wurden personenbezogene Kundendaten kompromittiert, diese kosten pro Datensatz 150 US-Dollar. Wenn die Daten bei einem böswilligen Angriff gestohlen wurden, steigen die Kosten nochmals um 17 Prozent auf 175 US-Dollar pro gestohlenen Datensatz.

Der „digitale Generalschlüssel“ im Dark Net: Immer mehr Daten in Form von E-Mailadressen, Usernamen und Passwörtern werden gestohlen. Allein 2019 waren es über 8,5 Milliarden gestohlene Datensätze. Zum Vergleich: Während der drei Jahre zuvor wurden insgesamt 11,3 Milliarden Daten gestohlen.

Die von IBM Security gesponserte und vom Ponemon Institut jährlich durchgeführte [„Cost of a Data Breach“](#)-Studie basiert auf ausführlichen Interviews mit mehr als 3.200 Sicherheitsexperten in Unternehmen, die im vergangenen Jahr eine Datenverletzung erlitten haben^[1]. Aus Deutschland haben 37 Unternehmen an der Studie teilgenommen.

Mehr Informationen und Studienergebnisse finden Sie in der ausführlichen US-Originalmeldung:

<https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year>

Die komplette **2020 „Cost of a Data Breach“-Studie** können Sie hier herunterladen:
<https://www.ibm.com/security/data-breach>

Bei Interesse können Sie sich auch für das kostenlose Webinar zur Studie anmelden. Dieses bieten wir am Mittwoch, der 12. August 2020 um 17:00 Uhr deutscher Zeit (US: 11:00 a.m. ET) an.

Anmeldung: <https://ibm.biz/BdqhMf>

Über IBM Security

IBM Security bietet eines der fortschrittlichsten und integritätstesten 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 70 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hält weltweit mehr als 10.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie [IBMSecurity](#) auf Twitter oder besuchen Sie den [IBM Security Intelligence blog](#).

^[1] Die Studie analysiert Datenpannen, die zwischen August 2019 und April 2020 aufgetreten sind.

For further information: IBM Unternehmenskommunikation Annette Fassnacht E-Mail:
annettefassnacht@de.ibm.com Telefon: +49-160 90105052

Additional assets available online:  [Photos](#) 
  

<https://de.newsroom.ibm.com/2020-07-29-Deutsche-Unternehmen-weltweit-fuehrend-bei-Security-Automatisierung>