NEWS RELEASE

ServiceNow-Studie: Trotz steigender Kosten, Schließen von Lücken bei der Datensicherheit dauert immer noch Wochen

2020-01-23

- Kosten für das Erkennen und Schließen von Schwachstellen in der Cyber-Sicherheit steigen in Deutschland gegenüber 2018 im Schnitt um mehr als 20 Prozent.
- Trotzdem dauert selbst das Beheben von kritischen Datenlecks immer noch fast 16 Tage.
- Mehr als 80 Prozent der IT-Experten in Deutschland sagen, dass eine Automatisierungslösung deutlich schnellere Reaktionszeiten ermöglicht.

München, 23. Januar 2020 – ServiceNow (NYSE: NOW) stellt das Ergebnis seiner Studie „Kosten und Konsequenzen von Verzögerungen bei der Bekämpfung von Schwachstellen der Datensicherheit“ für Deutschland vor: Trotz eines durchschnittlichen Anstiegs der jährlichen Ausgaben für Prävention, Erkennung und Behebung von Schwachstellen bei der Datensicherheit um 23,6 Prozent, dauert das Schließen von Datenlecks bei deutschen Unternehmen immer noch 15,92 Tage.

Damit schneiden die Deutschen im weltweiten Vergleich leicht besser ab. Global stiegen die Ausgaben um 24 Prozent und es vergingen im Schnitt 16,33 Tage, bis Datenlecks geschlossen werden konnten. Eine weitere gute Nachricht: Gegenüber der Umfrage in 2018 konnten die deutschen Unternehmen ihre Reaktionszeit um mehr als zwei Prozentpunkte verbessern. Die schlechte: Allein 11,4 der knapp 16 Tage von der Entdeckung bis zum Schließen eines Datenlecks gehen auf das Konto von Datensilos, unklaren Zuständigkeiten und schlechter organisatorischer Koordination. Gegenüber 2018 ist dieser Wert noch einmal leicht angestiegen.

Bedrohungslage bleibt aber kritisch

Im Schnitt stieg die Zahl der Cyberangriffe von 2018 auf 2019 in Deutschland um 17,1 Prozent (weltweit: 17 Prozent), die der schwere der Angriffe um 26,1 Prozent (weltweit: 26 Prozent). Die Untersuchung zeigt aber auch, dass fast 40 Prozent der befragten IT-Professionals sich über verwundbare Stellen ihrer Systeme im Klaren war, noch bevor es zum eigentlichen Datenleck kam. Mehr als 60 Prozent räumten ein, dass es für den ein oder anderen Vorfall einen Patch gegeben hätte, der aber nicht eingespielt worden war. Selbst die beste IT-Abteilung kann sich nicht zu 100 Prozent gegen Angriffe schützen.

„Mit den heute im Markt verfügbaren Automatisierungslösungen lässt sich sowohl die Performance beim präventiven Ausrollen von Patches klar erhöhen als auch die Reaktionszeit bei konkreten Vorfällen signifikant verbessern“, erklärt Detlef Krause, Area Vice President und General Manager Deutschland von ServiceNow. „Das bestätigen mehr als 80 Prozent der befragten IT-Experten in Deutschland, die heute schon solche Automatisierungslösungen in ihren Unternehmen einsetzen. Die Umfrageergebnisse unterstreichen also für Unternehmen in Deutschland die Notwendigkeit, ein effektiveres und effizienteres Management von Sicherheitslücken zu etablieren.“

Die wichtigsten Zahlen im Überblick (Prozentangaben im Vergleich zu den Angaben in 2018):

- 23,6% höhere Kosten für das Schließen von Sicherheitslücken (Patchen).
- 15,2 Tage dauert es im Schnitt, bis selbst kritische Schwachstellen behoben sind.
- 11,4 Tage davon sind unklaren Zuständigkeiten und mangelhaften organisatorischen Abläufen geschuldet.
- 18,6% mehr Ausfallzeiten aufgrund von Verzögerungen beim Patchen.

Die Zahl der Cyber-Attacken steigt weiter:

- 17,1% mehr Attacken als 2018
- 26,1% mehr kritische Attacken

Weitere Faktoren, die für Verzögerungen bei der Bearbeitung von Schwachstellen bei der Datensicherheit verantwortlich sind:

- 67% der Befragten klagt über die fehlende gemeinsame Sicht auf Anwendungen und Ressourcen in den unterschiedlichen IT-Teams.
- 86% der Befragten gibt an, dass sie kritische Anwendungen und Systeme nicht offline nehmen können, um sie schneller zu patchen.
- 88% der Befragten klagt über Schwierigkeiten bei der Priorisierung von Patches.

Über ServiceNow

ServiceNow (NYSE: NOW) schafft eine Welt, in der Arbeit weniger Arbeit macht. Unsere Cloud-basierte Plattform und die damit verbundenen Lösungen ermöglichen mit digitalen Workflows eine großartige User Experience, damit Mitarbeiter und Unternehmen effizienter arbeiten können. Für weitere Informationen besuchen Sie: **www.servicenow.com/de**.

Über ServiceNow Security Operations

Vulnerability Response ist Teil von ServiceNow Security Operations, einer Sicherheitsorchestrierungs-, Automatisierungs- und Reaktions-Engine, die auf der Now-Plattform basiert. Security Operations wurde entwickelt, um IT-Teams dabei zu unterstützen, schneller und effizienter auf konkrete Vorfälle und Schwachstellen bei der Datensicherheit zu reagieren. Dazu verwendet die Software intelligente Workflows, bietet Automatisierungsfunktionen an und ermöglicht eine tiefgreifende Integration in bestehende IT-Systeme.

© 2019 ServiceNow, Inc. Alle Rechte vorbehalten.