CROWDSTRIKE

CrowdStrike Global Security Attitude Survey

Die Kunden verlieren das Vertrauen in Legacy IT wie Microsoft, da Angriffe auf die Software-Lieferkette für Unternehmen ein zunehmendes Problem darstellen

68 %
der deutschen Befragten geben zu, dass ihr Unternehmen aufgrund der häufigen Sicherheitsvorfälle das Vertrauen in Anbieter wie Microsoft verliert

76 %
glauben, dass Angriffe auf die Software-Lieferkette innerhalb der nächsten drei Jahre zu einer der größten Cyber-Bedrohungen für Unternehmen wie das ihre werden könnten

45 % der befragten Unternehmen erlebten in den letzten 12 Monaten **mindestens einen Angriff auf die Software-Lieferkette**, verglichen mit **32 % im Jahr 2018**

2021

74 % der deutschen Befragten berichten, dass ihre Organisation schon einen **Angriff auf die Lieferkette** erlebt hat, **verglichen mit 32 % im Jahr 2018**

2018

Nur **40%**
der befragten deutschen Unternehmen haben alle neuen und bestehenden Lieferanten in den den letzten 12 Monaten einem Sicherheits-Check unterzogen

Ransomware ist nach wie vor weit verbreitet, wobei Auszahlungen und Erpressungsgebühren steigen

Die durchschnittliche geleistete Lösegeldzahlung deutscher Unternehmen betrug 1,38 Millionen Dollar, verglichen mit 1,09 Millionen Dollar im Jahr 2020

2021 **$1.38m**

2020 **$1.09m**

100%
der deutschen Unternehmen, **die das ursprüngliche Lösegeld bezahlt haben,** mussten zusätzlich **Erpressungsgebühren** in Höhe von durchschnittlich **542.593 Dollar** zahlen

Die durchschnittliche Lösegeldzahlung betrug **1,34 Millionen Dollar in EMEA, 1,55 Millionen Dollar in den USA** und **2,35 Millionen Dollar Millionen in APAC**

58%
der befragten deutschen Unternehmen **wurden mindestens einmal Opfer von Ransomware** in den **letzten 12 Monaten**

61%
der von Ransomware betroffenen Unternehmen **hatten keine umfassende Strategie** zur Koordinierung ihrer Reaktion

Die Unternehmen bewegen sich in die falsche Richtung, wenn es um die Erkennungs- und Reaktionszeit geht, weshalb die Security-Transformation priorisiert werden muss, insbesondere angesichts der Umstellung auf mobile und hybride Arbeitsmodelle

CrowdStrike ermutigt Organisationen zur Einhaltung der 1-10-60-Regel: Bedrohungen innerhalb der ersten Minute eines Angriffs erkennen, sie innerhalb von 10 Minuten analysieren und verstehen und innerhalb von 60 Minuten eindämmen und eliminieren.

	CrowdStrike Benchmark	Durchschnitt Umfrage 2021	Deutsche Ergebnisse 2021
Zeit bis zur **Entdeckung**	1 Minute	146 Stunden	120 Stunden
Zeit für die **Untersuchung**	10 Minuten	11 Stunden	8 Stunden
Zeit zur **Behebung**	60 Minuten	16 Stunden	15 Stunden

69 % haben einen Security-Vorfall erlitten, der direkt auf mobil arbeitende Teams zurückzuführen ist

Methodik

CrowdStrike beauftragte den unabhängigen Technologie-Marktforschungsspezialisten Vanson Bourne mit der Durchführung der quantitativen Untersuchung, auf der dieses Whitepaper basiert. Im September, Oktober und November 2021 wurden insgesamt 2.200 leitende IT-Entscheidungsträger und IT-Sicherheitsexperten in den Regionen USA, EMEA und APAC befragt. Sofern nicht anders angegeben, beziehen sich die diskutierten Ergebnisse auf die Antworten der deutschen Befragten (insgesamt 200).