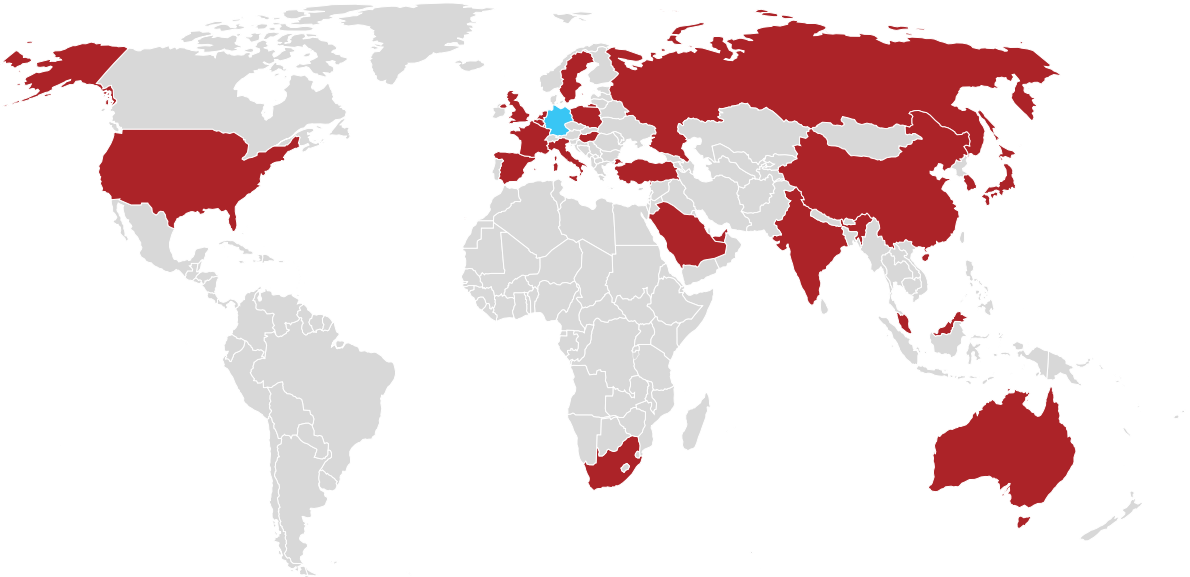
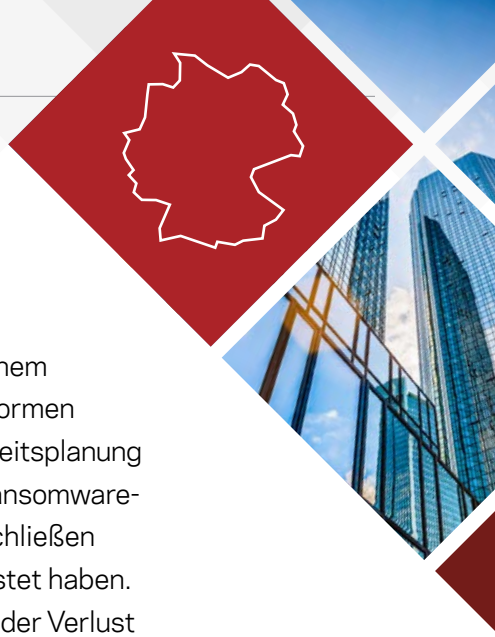
Veritas Ransomware Resiliency Research für Deutschland

Zusammenfassung der globalen Situation

Die globale Pandemie hat zur Beschleunigung der digitalen Transformation und insbesondere der Cloud-Implementierung beigetragen. Da Mitarbeiter jetzt von zu Hause aus arbeiten, werden mehr Daten im Unternehmen generiert und es besteht die geschäftliche Notwendigkeit, Anwendungen aus den firmeneigenen Rechenzentren in die Cloud zu verlagern. Eine neue globale Umfrage unter fast 2.700 IT-Führungskräften und -Experten in 21 Ländern, die von Wakefield Research im Auftrag von Veritas Technologies durchgeführt wurde, hat ergeben, dass mit der Beschleunigung dieses Wandels die Planung der Ausfallsicherheit nicht Schritt gehalten hat, sodass eine erhebliche Lücke entstanden ist. Dafür gibt es zahlreiche Gründe, aber der Schlüssel liegt darin, dass Unternehmen die Cloud zwar als eine leicht einzuführende Plattform für die Ausführung von Anwendungen und die Speicherung von Informationen empfunden haben, die Implementierung einer Plattform für die Ausfallsicherheit sich für viele jedoch als schwierig erwies. Es ist dringend erforderlich, dass Unternehmen diese Lücke in der Ausfallsicherheit schließen, indem sie ihre Planung beschleunigen, um mit dem heutigen Tempo und der zunehmenden Komplexität der IT Schritt zu halten.



VERITAS



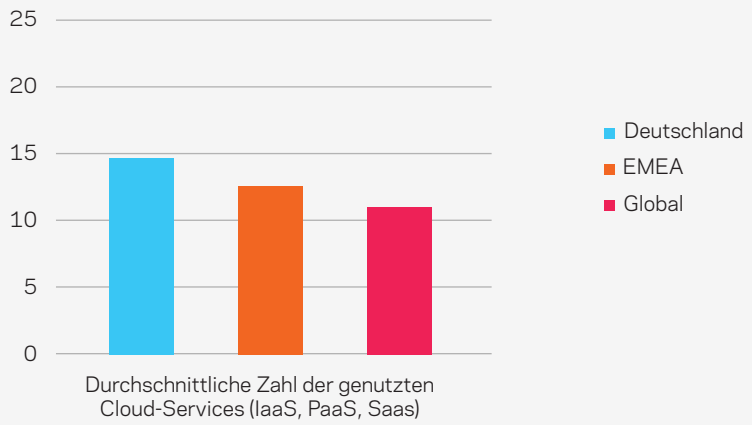
Deutschland – Ausblick

Viele deutsche Unternehmen sehen sich mit einer erheblichen Lücke in der Ausfallsicherheit konfrontiert, sodass ihre geschäftskritischen Daten leicht einem Ransomware-Angriff zum Opfer fallen können. Während sie mehr Cloud-Plattformen eingeführt und dadurch die IT-Komplexität erhöht haben, hat ihre Ausfallsicherheitsplanung nicht Schritt gehalten. Unternehmen in Deutschland erleben weniger häufig Ransomware-Angriffe als andere Unternehmen im EMEA-Raum und weltweit, was darauf schließen lässt, dass sie eine effektivere Arbeit zur Eindämmung dieser Bedrohung geleistet haben. Doch zu vielen von ihnen droht eine langwierige Geschäftsunterbrechung oder der Verlust von Daten, falls sie von einem Ransomware-Angriff betroffen sein sollten.

IT-Komplexität

- Im Vergleich zum weltweiten Durchschnitt stehen deutsche Unternehmen Cloud-Services sehr offen gegenüber. Ein durchschnittliches deutsches Unternehmen **nutzt ca. 15 Cloud-Services** (IaaS, PaaS und SaaS) und 23 % sogar mehr als 20. Ein durchschnittliches Unternehmen im EMEA-Raum nutzt hingegen **ca. 13 Cloud-Services**.

Wie viele Cloud-Services nutzt Ihr Unternehmen?



- Die verstärkte Cloud-Nutzung erhöht auch die IT-Komplexität. **76 % der Befragten in Deutschland gaben an, dass ihre Sicherheitsmaßnahmen mit der IT-Komplexität nicht Schritt halten.**

- Die größten Bedenken von deutschen IT-Führungskräften hinsichtlich der wachsenden IT-Komplexität sind sehr vielfältig und unterscheiden sich von denen ihrer Kollegen im EMEA-Raum:

Die größten Bedenken von deutschen IT-Führungskräften hinsichtlich IT-Überkomplexität:

35 % Höheres Risiko für interne Angriffe, wie Datenlecks, menschliches Versagen oder Dienstvergehen

34 % Höheres Risiko für externe Angriffe wie Datenpannen und Ransomware

33 % Mangelnde Transparenz von Daten und Anwendungen

Die größten Bedenken von IT-Führungskräften im EMEA-Raum hinsichtlich IT-Überkomplexität:

37 % Höheres Risiko für externe Angriffe wie Datenpannen und Ransomware

36 % Höheres Risiko für interne Angriffe (Datenlecks, menschliches Versagen, Dienstvergehen usw.)

35 % Potenzielles Risiko eines Datenverlusts

- Diese Bedenken werden noch dadurch verschärft, dass 61 % der deutschen Befragten angaben, dass die IT-Sicherheitsbudgets ihrer Unternehmen seit Beginn der COVID-19-Pandemie unverändert geblieben oder gesunken seien.

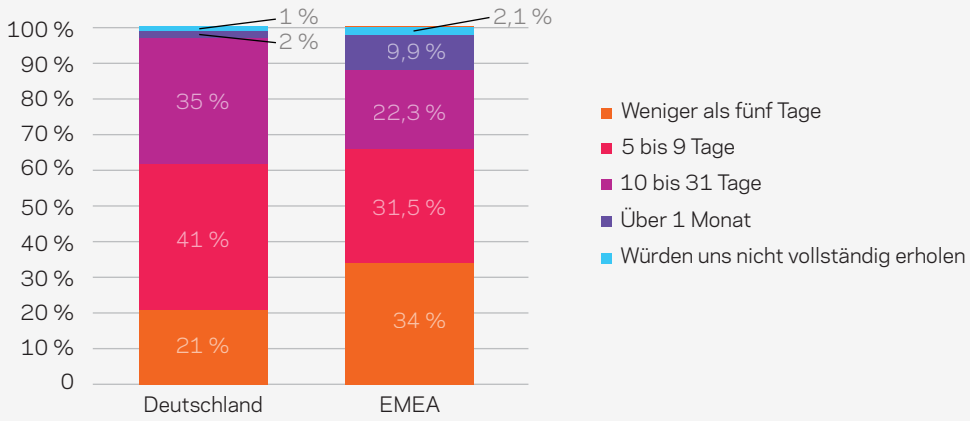
Auswirkungen von Ransomware

- Unternehmen in Deutschland wehren Ransomware-Bedrohungen im Vergleich zu ihren Kollegen im EMEA-Raum wirksamer ab. 27 % der deutschen Befragten gaben an, dass sie mit mindestens einem Angriff konfrontiert waren, gegenüber 38 % im gesamten EMEA-Raum.
- Zu viele Unternehmen in Deutschland zahlen den Preis dafür, dass ihre Ausfallsicherheit nicht ausreicht. Da ihre Backup- und Recovery-Systeme nicht robust genug sind, haben deutsche Unternehmen im Fall eines Ransomware-Angriffs oft keine andere Wahl, als das Lösegeld zu zahlen. Von denjenigen, die von einem solchen Angriff betroffen waren, gaben **60 % der deutschen Befragten an, dass ihr Unternehmen das Lösegeld ganz oder teilweise bezahlt hat**, im Vergleich zu 49 % im EMEA-Raum.

Lücke in der Ausfallsicherheit

- Deutsche Unternehmen sind sehr besorgt über ihre Fähigkeit, sich von einem Ransomware-Angriff zu erholen. **79 % der deutschen Befragten sind der Ansicht, dass es 5 Tage oder länger dauern würde**, bis sich ihr Unternehmen vollständig von einem Ransomware-Angriff erholt, wenn sie kein Lösegeld zahlen. Im Vergleich dazu gaben **65 % der EMEA-Befragten an**, dass eine vollständige Erholung von einem Ransomware-Angriff **5 Tage** dauern würde.

Wie lange würde es dauern, bis sich Ihr Unternehmen vollständig von einem Ransomware-Angriff erholt hat (wenn Sie kein Lösegeld gezahlt haben)?



- Nur 11 % der deutschen Befragten gaben an, dass sich ihr Unternehmen an die empfohlene Best Practice hält, drei Kopien ihrer Daten zu speichern, wobei eine Kopie extern und eine offline gespeichert wird. Weitere 37 % der deutschen Befragten gaben an, ihr Unternehmen habe drei oder mehr Kopien ihrer Daten vor Ort gespeichert.
- Deutsche Unternehmen testen ihre Disaster Recovery-Pläne regelmäßiger als ihre globalen Kollegen: 74 % haben ihn in den letzten drei Monaten getestet, verglichen mit 60 % der weltweiten Unternehmen. Dennoch glauben sie, dass 23 % ihrer Daten nicht wiederherstellbar wären, falls sie durch Ransomware den Zugriff darauf verlieren.

Empfehlung für deutsche Unternehmen: Unternehmen in Deutschland wehren Ransomware-Bedrohungen wirksam ab, aber es gibt noch genug Risiken. Die Tatsache, dass sechs von zehn deutschen Unternehmen, die einen Ransomware-Angriff erlebt haben, das Lösegeld zahlten, deutet darauf hin, dass diese Unternehmen sich mehr auf die Planung der Ausfallsicherheit konzentrieren müssen. Die Unternehmen in Deutschland müssen sich so schnell wie möglich um die Lücke in der Ausfallsicherheit kümmern, damit sie ihre Daten wiederherstellen können, ohne das Lösegeld zu zahlen. Sie sollten robustere Methoden zur Abwehr von Ransomware-Bedrohungen einführen, beispielsweise:

- **Durchgängige Überprüfung der Strategie:** Deutsche Unternehmen sollten ihre Ausfallsicherheitsstrategie überprüfen, um zu gewährleisten, dass sie planbar ist und auf Echtzeit-Transparenz, Überwachung und Automatisierung der Wiederherstellung basiert.
- **Robusteres Backup:** Unternehmen sollten einen „3-2-1"-Backup-Ansatz verfolgen: mindestens drei Kopien ihrer Daten an zwei verschiedenen Orten speichern, von denen einer extern ist.
- **Häufigere Disaster-Recovery-Tests:** Idealerweise sollten Unternehmen ihren DR-Plan einmal pro Monat testen. Die Daten- und Anwendungslandschaft ändert sich so schnell, dass bei weniger häufigen Tests die Gefahr besteht, dass ein DR-Standort ausfällt, wenn er benötigt wird.
- **Häufige Sicherheitsupdates:** IT-Teams sollten Sicherheitspatches und neue Versionen mit Sicherheitsupdates nach ihrer Veröffentlichung so bald wie möglich installieren.
- **Datenverschlüsselung:** Unternehmen sollten ihre Datenübertragungen verschlüsseln, um sie vor Kompromittierung im Netzwerk zu schützen.
- **Unveränderlicher Speicher:** IT-Teams sollten unveränderliche und unlöschbare Speichertechnologie verwenden, um zu verhindern, dass Ransomware Backups verschlüsseln oder löschen kann.
- **Zugriffsverwaltung:** Implementieren Sie eine rollenbasierte Zugriffssteuerung und beschränken Sie den Zugriff für Einzelpersonen und Rollen auf die erforderlichen Funktionen.