

VMware Bericht warnt vor Deepfake-Angriffen und Cyber-Erpressung

Vorsicht vor Deepfakes

Cyberkriminelle setzen bei ihren Angriffen vermehrt auf Deepfakes.



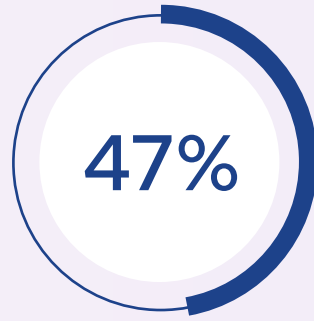
66%
der Incident-Responders bezeugen Deepfake-Angriffe in den letzten 12 Monaten



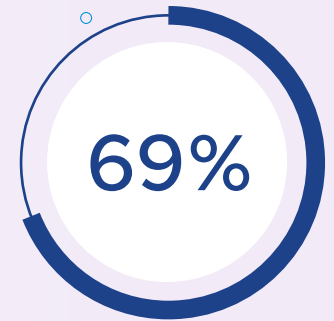
78%
der Incident-Responders identifizieren E-Mail als Übertragungsmöglichkeit, was mit der Kompromittierung von Geschäfts-E-Mails einhergeht.

Die Überlastung von Sicherheitsteams ist ein massives Problem

Organisationen führen Wellness-Programme ein, um einen Ausgleich zum stressigen Arbeitsalltag zu schaffen. Dennoch bleibt Burnout unter den Incident-Responders ein Thema.



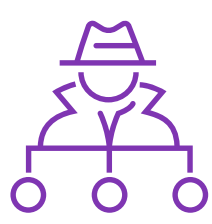
47%
litten unter Burnout oder extremen Stress innerhalb der letzten 12 Monate



69%
zogen deswegen in Erwägung, ihren Job zu kündigen

Die Zunahme von Cyber-Erpressungen

Ransomware Gruppierungen verfolgen mit Ransomware noch hinterhältigere Ziele: Cyber-Erpressungen.



66%
der Incident-Responders stießen auf Affiliate-Programme oder Partnerschaften zwischen Ransomware-Gruppen

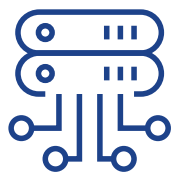


25%
der Ransomware-Angriffe umfassten Techniken der Doppelerpressung

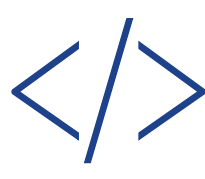
APIs sind der neue Endpoint

Mit der Zunahme an Workloads und Anwendungen kompromittieren 23% der Angriffe die API-Sicherheit.

Die häufigsten Arten von API-Angriffen sind:



Data exposure (42%)



SQL- und API-Injection-Angriffe (37%)



API-Injection-Angriffe (34%)



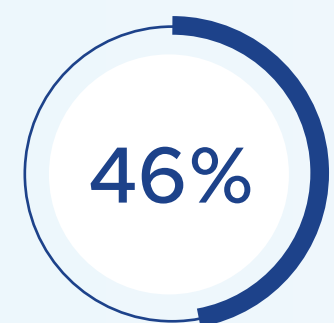
Distributed Denial-of-Service Angriffe (33%)

Laterale Bewegungen sind die neue Angriffsfläche

Angreifer warten ab, bleiben bei den allgemeinen Netzwerkkaktivitäten unbemerkt und nutzen gängige Ports und Protokolle, um Schaden anzurichten.



25%
der Angriffe setzten auf laterale Bewegungen



46%
nutzten Dateispeicher- und Synchronisierungstools zum durchsuchen von Netzwerken

Neue Abwehrtechniken

Sicherheitsteams passen ihre Strategien an, um erfolgreich zu verteidigen.



87%
der Incident-Responders unterbrechen manchmal oder sehr oft die Aktivitäten von Cyberkriminellen



75%
der Incident-Responders setzen virtuelle Patches als Notfallmechanismus ein

Best Practices für mehr Sicherheit



Ganzheitlicher Fokus auf Workloads



Kontrolle des In-Band-Traffics



Integration von NDR in EDR



Einsatz von Zero-Trust-Ansätzen



Kontinuierliches Threat-Hunting

Methodik

VMware führte im Juni 2022 eine Online-Umfrage zu Trends in der Incident-Response-Landschaft durch, an der 125 Cybersicherheits- und Incident-Response-Experten aus der ganzen Welt teilnahmen.