BOMGAR™

SICHERER ZUGRIFF OHNE VPN

Bomgar Privileged Access Management bietet Ihnen die Möglichkeit, Zugriffe auf wichtige Systeme durch privilegierte Nutzer, externe Dienstleister oder Lieferanten zu steuern, zu überwachen und zu verwalten.
Mit Bomgar können Sie:

- die Angriffsfläche für potentielle Hacker deutlich reduzieren
- Zugriffe auf Ihr Netzwerk detailgenau kontrollieren
- Sessions in Echtzeit überwachen und auditieren
- Session Logs direkt in Ihr SIEM-Tool übernehmen und auswerten
- Angriffe mit Identitätsmissbrauch wirkungsvoll unterbinden
- Reaktionszeiten bei Incidents verkürzen
- Forensische Untersuchungen effektiv durchführen
- Audit- und Compliance-Vorgaben erfüllen

BOMGAR.COM/DE

Wussten Sie schon?

Hacker benötigen in der Regel Tage und Wochen, bis sie das Gesuchte finden. Erhalten sie VPN-Zugriff zu einem internen Netzwerk über ein angegriffenes System, können sie sich dort oft unerkannt bewegen und Pivoting-Methoden einsetzen, um ihr endgültiges Ziel zu finden. Hacker greifen oft externe Anbieter mit veralteten Zugangsmethoden wie VPN und RDP zu einem sicheren Netzwerk an, da diese leicht zu kompromittieren sind. Bomgar gibt Lieferanten genau den Zugang, den sie benötigen – sicher und ohne VPN. Hierdurch wird das Risiko gehackter Lieferanten-VPNs ausgeschlossen.

dauert es im Durchschnitt, bis ein Hacker-Angriff entdeckt wird. Wurde ein Lieferantenzugang kompromittiert, wird im Falle von Bomgar jegliche schädliche Aktivität gestoppt, sobald die Bomgar-Sitzung beendet wurde bzw. abläuft. Bei einem VPN-Zugang hingegen kann sich der Hacker so lange frei bewegen, bis er erkannt wird.

80 % aller Angriffe betreffen privilegierte Nutzerkonten. Sie haben keine Kontrolle über das Sicherheitsdenken Ihrer Lieferanten. Für einen Hacker sind Ihre Lieferanten in der Regel eine einfachere und praktische Möglichkeit, Ihr Netzwerk anzugreifen.

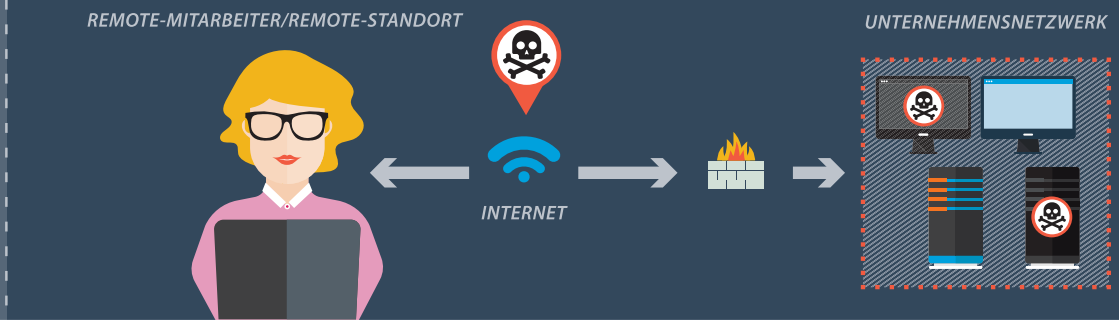
62%

aller Unternehmen halten die Identitäts- und Zugriffsrechteverwaltung innerhalb ihrer Organisation für zu schwierig und aufwändig. Unternehmen haben im Durchschnitt über 300 Informationsressourcen und 1.200 Zugriffsanfragen pro Monat. Bomgar reduziert diese Komplexität, indem Administratoren erlaubt wird, Systemzugriffe zentral zu verwalten, zu überwachen und zu auditieren, ohne die Prozesse zu unterbrechen.

GEBEN SIE LIEFERANTEN ZUGANG OHNE VPNS!

VOR LANGER, LANGER ZEIT ...

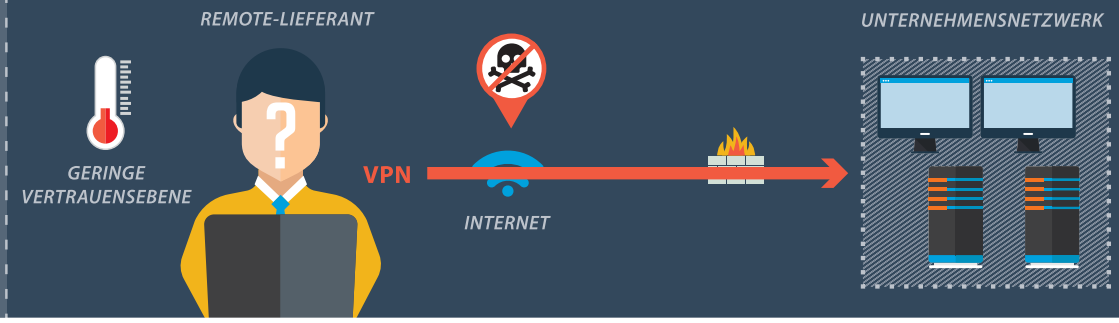
bestand das größte Sicherheitsrisiko in einem MItM-Angriff (Man in the Middle) auf eine Remote-Verbindung zu Ihrem Netzwerk.



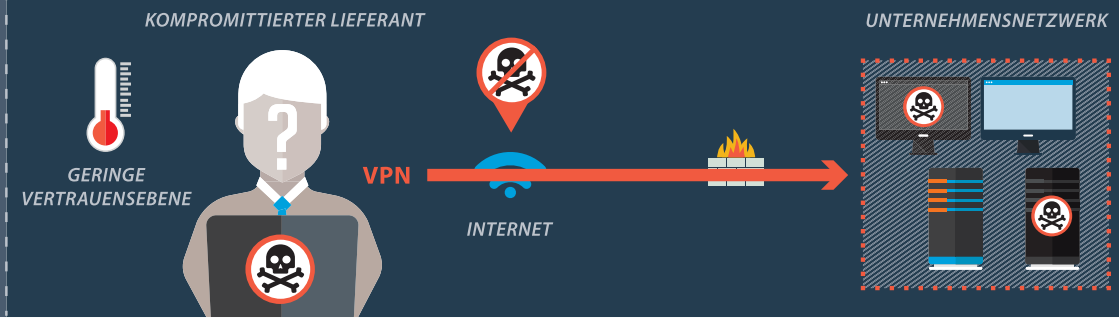
Um die MItM-Angriffe zu unterbinden, begannen Unternehmen mit der Implementierung von VPNs um verschlüsselte Tunnel für den Netzwerkzugriff von Remote-Mitarbeitern und Remote-Standorten bereitzustellen.

AUßER KONTROLLE!

Im Laufe der Zeit benötigten aber auch externe Parteien und Lieferanten privilegierten Zugang zum internen Netzwerk. Hierfür setzten Unternehmen auf das beste Tool, das sie kannten – VPNs

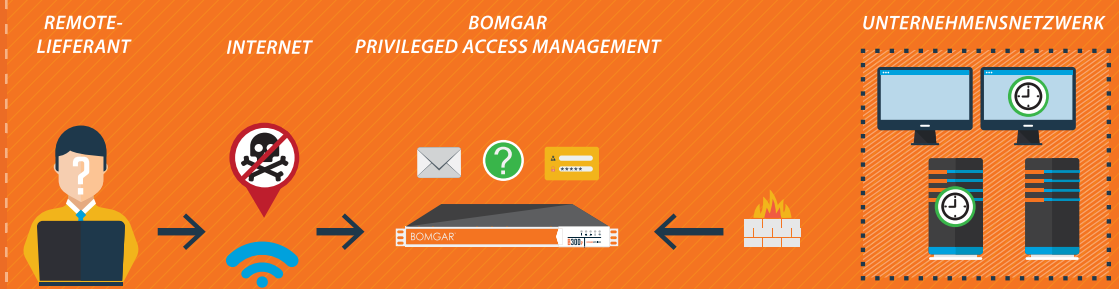


Internetkriminelle entdeckten dies schnell für sich: Lieferanten mit VPN-Verbindung sind das perfekte Ziel, um Zugang zu einem sicheren Netzwerk zu erhalten. Mit einem VPN-Zugang haben sie die Zugriffsmöglichkeit und alle Zeit der Welt, sensible Systeme zu finden und anzugreifen.



GEBEN SIE LIEFERANTEN ZUGANG OHNE VPN!

Mit Bomgar Privileged Access Management können Sie Lieferanten Zugang zu Ihrem Netzwerk gewähren – ganz ohne VPN-Verbindung und ohne Direktverbindung zu Ihren wertvollsten internen Systemen, das Ziel der Hacker.



MitM-Angriffe werden nach wie vor verhindert.

Bomgar ermöglicht Ihnen, granulare Zugriffsberechtigungen zu gewähren oder Genehmigungen für den Lieferantenzugriff anzufordern. Zudem erstellt das System einen durchsuchbaren Audit-Trail sowie Videoaufzeichnungen aller Anbieteraktivitäten.

Keine Firewall-Modifizierungen erforderlich. Der externe Anbieter ist nur über eine ausgehende Verbindung mit der Bomgar-Appliance verbunden, NICHT mit dem Zielsystem.

Mit Bomgar können Sie genau festlegen, auf welche Systeme, wann und für wie lange die Lieferanten zugreifen dürfen. Längere Aufenthalte in Ihrem Netzwerk werden auf diese Weise ausgeschlossen. Mit uns sind Advanced Persistent Threats nicht länger „Persistent".