Wie Ransomware ungeschützte Remote-Desktop-Protokolle ausnutzt

Wie groß ist das Problem?

768%
mehr RDP-Angriffe zwischen Q1 und Q4 2020[1]

47%
der Bedrohungsakteure, die Ransomware einsetzen, haben sich 2020 RDP zunutze gemacht[2]

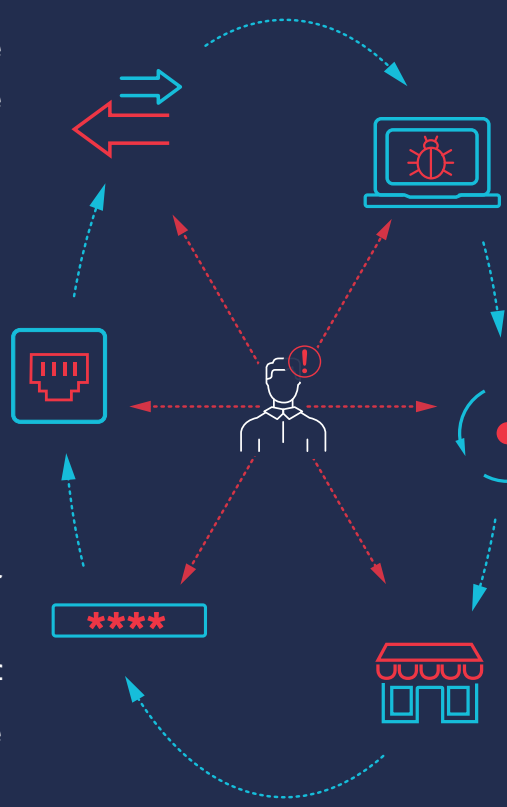
4.7 Millionen
fehlkonfigurierte RDP-Rechner sind laut Coveware offen für einen Zugriff über das Internet[3]

Was ist die Ursache für diese Angriffe?

RDP ist die beliebteste Technologie für die Verbindung zu Remote-Systemen

RDP-Ports werden im Internet offen gelassen und sind mit einfachen Passwörtern zugänglich

Kompromittierte Passwörter führen zu unberechtigten Zugriffen auf Unternehmensnetzwerke



Es gibt Millionen von Computern mit offenen RDP-Ports

RDPs werden für verschiedene schädliche Cyber-Aktivitäten verwendet, darunter Ransomware-Angriffe

Kriminelle verschaffen sich über "RDP-Traffic-Seiten" kostenlos Zugriff

Was lässt sich dagegen tun?

Vermeiden Sie die Veröffentlichung ungeschützter Remote-Desktops im Internet und schützen Sie den Zugangspunkt mit MFA

Nutzen Sie RDP-Gateways – Reverse-Proxy-Gateways verschleiern den Port

Nutzen Sie MFA für den Zugriff auf das RDP-Gateway

Nutzen Sie MFA auch für die Netzwerkanmeldung, sobald Sie auf den Remote-Desktop zugegriffen haben

Folgen Sie uns auf:

THALES
Building a future we can all trust

1 https://www.netsec.news/rdp-attacks-increased-by-768-in-2020-and-remain-a-key-attack-vector
2 https://www.lexology.com/library/detail.aspx?g=30323e3e-7660-4e5e-af70-5d2b8df2ec57
3 https://www.coveware.com/blog/2020/10/14/state-and-local-cybersecurity-defending-our-communities-from-cyber-threats-amid-covid-19