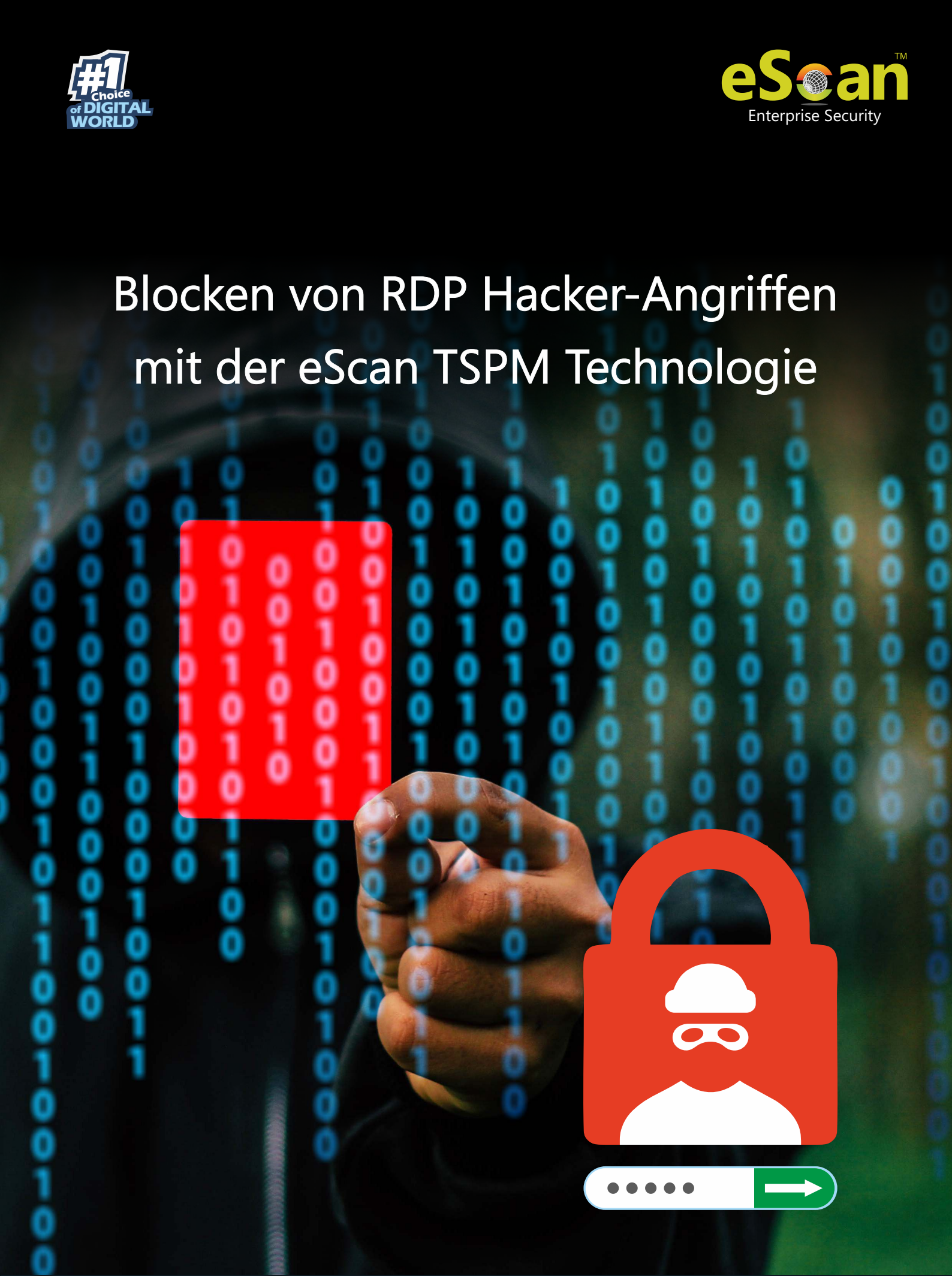
#1 Choice of DIGITAL WORLD

eScan™
Enterprise Security

Blocken von RDP Hacker-Angriffen mit der eScan TSPM Technologie



eScan startet die neue TSPM Technologie zum Blocken von RDP Hacker-Angriffen

Mit der steigenden Komplexität von Cyberangriffen müssen Unternehmen Millionen ausgeben, um Cyberkriminalität abzuwehren. Durch schlechte Sicherheitspraktiken wie Verwendung einfacher Passworte für den Systemzugriff werden den Cyberkriminellen Gelegenheiten zum Eindringen gegeben. In solchen Szenarien verwenden Cyberkriminelle Brute-Force Angriffe, um Kontrolle des Netzwerkes zu übernehmen. Basierend auf dem "National Exposure Index" Bericht von Rapid7 sind 73% der indischen RDP Server bloßgestellt für Brute-Force Angriffe und stehen weltweit hiermit auf Platz 18.

In den letzten zwei Monaten beobachtete eScan, dass die meisten Ransomware Angriffe dazu beitragen könnten, dass Cyberkriminelle mit schurkischen RPD Sitzungen die Kontrolle von Servern übernehmen und Ransomware starten können, um Lösegeld von den Firmen zu erpressen. Hierbei werden dann alle möglichen Schritte unternommen, um den Echtzeitmonitor abzuschalten und/oder jegliche Antischadsoftware-Produkte auf den entsprechenden Endgeräten zu deinstallieren.

IT Administration und Anlagenverwaltung ist eine langwierige Aufgabe. Zur Vereinfachung des Prozesses der Fehlersuche/Wartung verwenden IT Administratoren verschiedene Fernzugriffstechnologien, z.B. das Remote Desktop Protocol (RDP), um auf das grafische Interface eines anderen Computers über das Netzwerk zuzugreifen.

Es ist zu beachten, dass die Sicherheit von RDP begrenzt ist auf komplexe Passworte und eine sichere Verbindung durch die Implementation von TLS, um die verschiedenen Formen von Brute-Force/Passwortrate-Angriffen oder MITM Angriffen zu entschärfen.

Aus verschiedenen Gründen implementiert nicht jedes Unternehmen Passwortrichtlinien und in vielen Fällen darf der Benutzer sein eigenes Passwort wählen. Weiterhin ist die Wiederverwendung des Passwortes ein Bedenken, dass angesprochen werden muss.

Verwendung von RDP

Zur Durchführung der zentralen Verwaltung von Computern implementieren Unternehmen RDP und greifen auf diese Systeme über LAN oder Internet zu. Um Systeme, bei denen RDP freigeschaltet ist, von außen zu schützen, kann VPN eingerichtet werden, aber in den meisten Fällen konfigurieren Administratoren die Firewall zum Öffnen von RDP für die Systeme, die sie aus der Ferne verwalten wollen

RDP Angriffe

Penetrationstest-Plattformen wie Kali bieten RDP Brute-Force- und Exploit-Werkzeuge, die speziell verwendet werden für RDP-Systeme, die vom Internet her offen sind. Brute-Force Angriffe erzeugen eine große Anzahl von fehlgeschlagenen Anmeldungsbenachrichtigungen und werden aufgezeichnet. Benutzer bekommen von den laufenden Brute-Force Angriffen kaum etwas mit, da sie während des Angriffs nicht eingeloggt sein oder an dem System arbeiten müssen.

- Auch wenn fehlgeschlagene RDP Authentifizierungen aufgezeichnet werden, erhält der Benutzer nie eine Warnung, wenn die Sicherheit erfolgreich verletzt wurde. Das Resultat ist eine Zunahme von Brute-Force auf RDP-Sitzungen.
- Auf Grund der Tatsache, dass Benutzer nie etwas von den dauernden RDP Authentifizierungen mitbekommen, erlangt der Eindringling komplette Kontrolle über das System.
- Nach dem erfolgreichen Eindringen installieren die Angreifen Backdoors oder gelangen auf andere System und in einigen Fällen infizieren sie die Systeme mit Ransomware.

TSPM – Terminal Services Protection Modul

eScans Terminal Services Protection Modul (TSPM) erkennt nicht nur diese Brute-Force Angriffe sondern identifiziert die verdächtigen IP-Adressen/Hosts und blockt jegliche Zugriffsversuche von ihnen und, um die Systeme vor zukünftigen Angriffen zu schützen, verbietet den IP-Adressen und Hosts weitere Verbindungen zu dem System.

Wie bereits zuvor erwähnt, ist es bekannt geworden, dass Angreifer versuchen, die Sicherheitsanwendungen auf den bloßgelegten Systemen zu deinstallieren, damit ihre Spuren unerkannt bleiben und Administratoren keine Warnung über das Eindringen erhalten. eScan TSPM erkennt und stoppt solche Versuche und meldet dem Administrator die präventiven Maßnahmen, die von TSPM eingeleitet wurden.

In der heutigen IT-Landschaft, in der Angreifer versuchen, jede bekannte Schwachstelle zu öffnen – seien es ungepatchte Systeme oder die Unfähigkeit von Benutzern/Administratoren zur Einhaltung von Passwort-Hygiene –, schützt eScans TSPM die Systeme/Unternehmen vor solchen Angriffen.