# Kurzanleitung für *CSC Security Center*

**Da Cyber-Angriffe mittlerweile alltäglich stattfinden und weiter zunehmen, ist es wichtiger denn je, dass diejenigen, die mit der Verteidigung der Online-Präsenz einer Marke beauftragt sind, die richtigen Partner und Tools für diese Aufgabe auswählen.**

Digitale Assets sind bekanntermaßen eine Schwachstelle, die von Cyber-Kriminellen und Hackern ausgenutzt wird. Daher reicht es nicht mehr aus, sich für einfache Verwaltungsdienste zu entscheiden und die Vorgehensweise einfach jährlich zu überprüfen.

Um Cyber-Kriminellen einen Schritt voraus zu sein und Markeninhabern bei ihren sich schnell entwickelnden Geschäftsmodellen zu helfen, hat CSC das Tool CSC Security Center℠ entwickelt, das die Komplexität beseitigt und die Kontrolle zurück in die Hände unserer Kunden legt.

## Wo liegen die Risiken und wie hilft mir CSC Security Center?

Mithilfe mehrerer Datenquellen und eines komplexen Algorithmus, der bei einigen der weltweit größten Unternehmen getestet wurde, kann CSC Security Center Ihre geschäftskritischen digitalen Assets identifizieren und überwachen und damit eine laufende Risikobewertung bereitstellen. So können Sie die potenziellen Gefahren eines Cyber-Angriffs auf die überwachten Assets sofort erkennen und abwehren.

| Risiken | Folgen | Auswirkung | CSC-Lösung |
|---|---|---|---|
| **Mangelhafte Kontenführung und Verwaltung** | Ablauf von geschäftskritischen Domains und digitalen Zertifikaten (SSL) | Keine Website-Namensauflösung, keine E-Mail, kein virtuelles privates Netzwerk (VPN) oder Voice-over-IP (VoIP); Verlust des Kundenvertrauens und möglicherweise Anfälligkeit für einen Malware- oder Ransomware-Angriff | Überprüfung und Konsolidierung von Domains, des Domain Name Systems (DNS) und digitaler Zertifikate (SSL) |
| **Fremd-Provider** | Social Engineering, Phishing oder Distributed Denial of Service (DDoS)-Angriff | Verlust der Kontrolle über Website-Auflösung, E-Mail, VPN oder VoIP und die Möglichkeit, dass Cyber-Kriminelle Websites klonen und E-Mails stehlen | Fokus auf Sicherheit; wir investieren stark in Technologie und Personal |
| **Zugänglichkeit von Assets** | Social Engineering, Phishing-Angriff | Verlust der Kontrolle über Website-Auflösung, E-Mail, VPN oder VoIP und die Möglichkeit, dass Cyber-Kriminelle Websites klonen und E-Mails stehlen | Sicherung des Zugriffs auf das Verwaltungssystem durch IP-Validierung, Zwei-Faktor-Authentifizierung und föderierte Identität |
| **Bedrohungen durch Dritte** | Versäumnisse bei der Eindämmung von DDoS- und Phishing-Angriffen | Keine Website-Namensauflösung, kein E-Mail, VPN oder VoIP – dient als Nebelwand für einen zweiten Angriff | Sicherung der Assets vor den bekannten Bedrohungen mit MultiLock, DDoS-Abwehr, E-Mail-Authentifizierung und Anti-Phishing-Serviceleistungen |
| **Statischer Ansatz** | Nicht identifizierte geschäftskritische Domains und Risiken | Verlust der Kontrolle über Website-Namensauflösung, E-Mail, VPN oder VoIP und die Möglichkeit, dass Cyber-Kriminelle Websites klonen und E-Mails stehlen | CSC Security Center |