Sicherheit digitaler Assets:

Zurück zu den Grundlagen

Sicherheit digitaler Assets: *Zurück zu den Grundlagen*

Die vielen Cyber-Angriffe und Datenschutzverletzungen weltweit zeigen, dass die Vorfälle an Zahl und Intensität zunehmen und es immer komplizierter wird, die Umgebung zu schützen. Unternehmen investieren zwar weiterhin in Technologie, doch nehmen die Herausforderungen beim Schutz von Unternehmen täglich zu.

Viele derzeitige Sicherheitsmethoden, -Tools und -Techniken, mit denen Unternehmen versuchen, ihre Umgebung zu sichern und ihre Marke zu schützen, waren zwar bislang effektiv, aber die Angriffe kommen inzwischen aus allen Richtungen. Hacker, Hacktivisten, Cyber-Kriminelle, Staaten und Insider (etwa Mitarbeiter) arbeiten alle daran, eine Schwachstelle in den Sicherheitsprotokollen zu finden, um in Systeme zu gelangen.

Unternehmen, die wissen, dass Daten über verschiedene Eingangspunkte hereinströmen, aber immer noch zwischen innerer und äußerer Sicherheit unterscheiden, sollten dringend ihren Sicherheitsansatz – insbesondere die Rolle ihrer digitalen Assets (also Domains, Domain Name System (DNS) und digitale Zertifikate) – bei der Sicherung des alltäglichen Betriebs ihrer Geschäfte überdenken.

Aber wie kann ein Umstieg von einem herkömmlichen Cybersicherheits-Ansatz zu einem, der die heutigen Risiken tatsächlich vermindert, aussehen?

Die digitalen Assets verstehen und identifizieren, um sie richtig verwalten zu können.

Die Auswirkungen eines Vorfalls für das Unternehmen erfassen und entsprechend planen.

Den ROI optimieren. Wissen, was wichtig ist (zum Beispiel wesentliche Domains) und was nicht.

Die vielen digitalen Kanäle verteidigen.

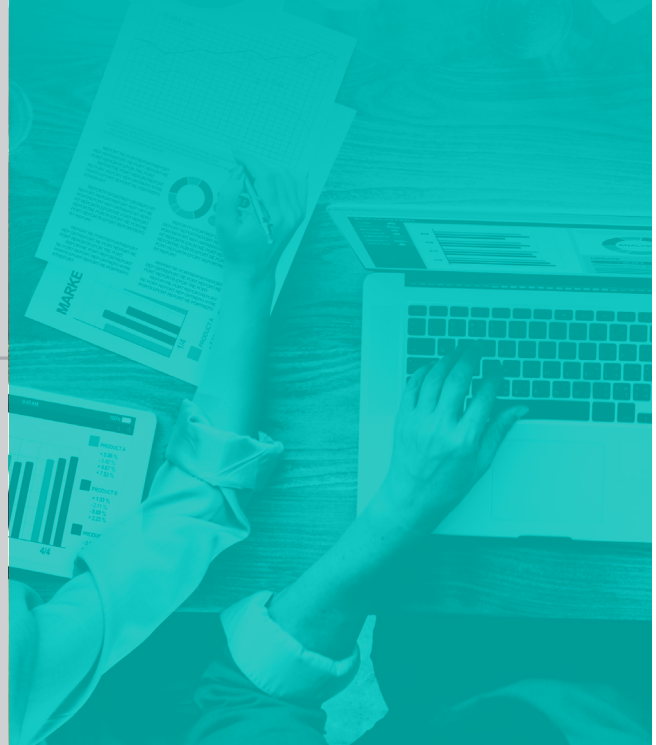
1

2

3

4

Die digitalen Assets verstehen und identifizieren, um sie richtig verwalten zu können.



Im Verlauf der letzten 20 Jahre hat Ihr Unternehmen eine große Anzahl digitaler Assets angesammelt. Diese digitalen Assets stellen Ihre Firma vor und dar, ermöglichen die Durchführung von Transaktionen und sichern eine reibungslose Kommunikation und Interaktion mit Kunden, Zulieferern und Kollegen. Kurz gesagt, sie haben die Art und Weise, wie Sie kommunizieren, arbeiten und konsumieren, verändert.

Die Welt ist heute mehr denn je miteinander verbunden – und obwohl dies eine fantastische Gelegenheit für Unternehmen auf der ganzen Welt ist, bringt dies Leerzeile entfernen mit sich. Mit der Entwicklung der globalen digitalen Wirtschaft entwickeln sich auch Online-Assets wie Domainnamen, digitale Zertifikate (SSL), Social Media-Nutzernamen und mobile Apps weiter. Deshalb müssen Unternehmen unbedingt wissen, welche Online-Assets sie besitzen und nutzen. Andernfalls ist das Unternehmen anfällig für Markenrechtsverletzungen und Cyber-Angriffe.

Wahrscheinlich sind die Informationen darüber, was im Besitz ist und was tatsächlich verwendet wird, über verschiedene Abteilungen, z. B. Marketing, Recht, IT und manchmal sogar einzelne Personen, verstreut. Deshalb ist es am besten, mit der Erstellung einer Liste aller Online-Assets zu beginnen und Ihre Provider und Registrare um die Durchführung einer Überprüfung zu bitten. Jedes Unternehmen muss ganzheitlich an die Sache herangehen. Wenn Sie etwa in den USA arbeiten, dann müssen Sie sich trotzdem die Online-Assets in allen Regionen ansehen, in denen Ihr Unternehmen tätig ist.

Checkliste: Folgendes sollten Sie feststellen

- ○ **Die Domainnamen in Ihrem Besitz, auch die für Werbezwecke (wie Vanity-URLs) oder aus Abwehrgründen registrierten Domains**
- ○ **Wer stellt das DNS für die einzelnen Domains zur Verfügung, sei es Ihr Domain-Registrar, ein spezieller DNS-Anbieter oder eine Infrastruktur, die Sie selbst verwalten und unterstützen**
- ○ **Die Anzahl der vorhandenen digitalen Zertifikate (SSLs), einschließlich der jeweiligen Art der Validierung und ihrer Verwaltung**
- ○ **Die Anzahl von Profilnamen auf den verschiedenen sozialen Medien**
- ○ **Wer hat Zugang zu den Benutzernamen und Passwörtern in sozialen Medien und wie werden die Profilnamen verwaltet**
- ○ **Haben Sie mobile Apps entwickelt und veröffentlicht und wie werden diese verwaltet**

Bei der Zusammenstellung dieser Informationen ist es auch wichtig, einen Überblick darüber zu gewinnen, wer Zugriff hat und wozu.

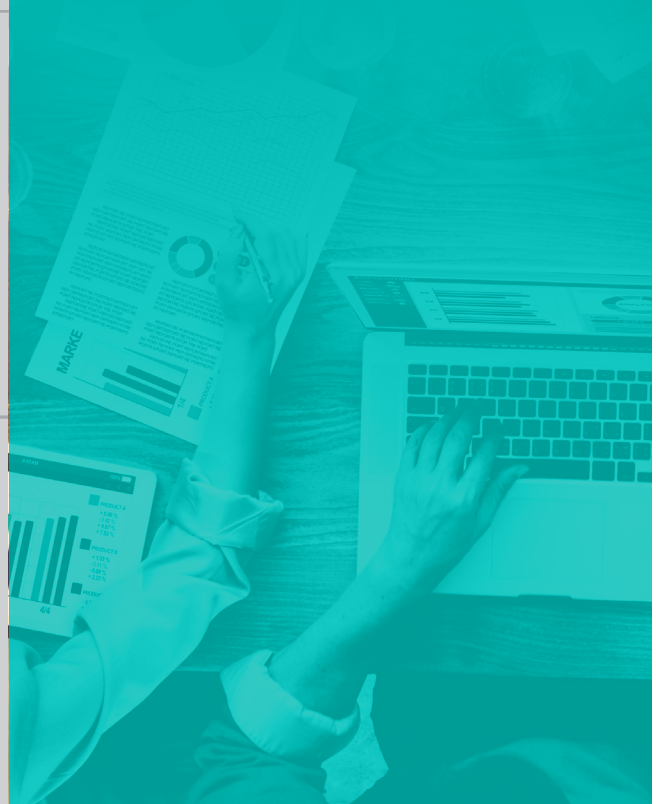
1

2

3

4

Die digitalen Assets verstehen und identifizieren, um sie richtig verwalten zu können.



Konsolidieren Sie Ihre Online-Assets bei Enterprise-Class-Providern

Durch ein Verständnis der Erfordernisse Ihres globalen Geschäftsbetriebs in Bezug auf Domains, DNS und digitale Zertifikate stellen Sie sicher, dass jeder Provider, mit dem Sie arbeiten, die erforderlichen Kriterien erfüllt. Für jeden Bereich gibt es eine breite Vielfalt von Providern, von kostengünstigen „DIY“-Providern mit begrenzten Serviceangeboten und Abrechnung über Kreditkarten bis hin zu Enterprise-Class-Providern mit erstklassigem Service sowie SLA, Haftung und den richtigen Abrechnungsmodellen für ein globales Unternehmen. Auch die Einstellung des gewählten Partners zur Sicherheit muss in die Überlegungen unbedingt mit einbezogen werden.

Neben der sorgfältigen Prüfung der Qualität Ihrer Provider empfiehlt es sich außerdem, Ihre Online-Assets zu konsolidieren, um eine reibungslose Verwaltung und Business Continuity zu gewährleisten. Wenn Sie in der Lage sind, alle Ihre Online-Assets durch ein eigens dafür aufgestelltes Team – und idealerweise auf nur einer Plattform – zu verwalten, können Sie besser auf Änderungen reagieren. Dazu gehören die Registrierung oder der Verfall von Domainnamen, Änderung von Social Media-Anmeldedaten, Erneuerung digitaler Zertifikate (SSLs) und vieles mehr. Vor allem aber erhalten Sie dadurch einen klaren Überblick über Ihre Sicherheitsschwachstellen.

Bitten Sie zukünftige oder aktuelle Provider, eine Überprüfung Ihrer Online-Assets vorzunehmen.

Arbeiten Sie mit einem Enterprise-Class-Provider zusammen, wenn dies bislang noch nicht der Fall ist. Sie können Ihnen sicher die bestmögliche Verwaltung digitaler Zertifikate, Domains und DNS bieten. Sie dürften auch in der Lage sein, alle von ihnen verwalteten Domains zu überwachen, um so Ihre Leerzeile entfernen hinsichtlich DNS und digitaler Zertifikate durchzusetzen. Einige der Fragen, die unbedingt beantwortet werden müssen, sind: Leerzeile löschen sind nicht aktiv oder führen nicht zum gewünschten Inhalt? Welche geschäftskritischen Domainnamen verwenden keine DNSSEC-Erweiterungen (Sicherheitserweiterungen des Domainnamensystems)? Und ist „SSL Always On“ bei Ihren geschäftskritischen Domains aktiviert?

Mindestens diese Art von Überprüfung sollte regelmäßig durchgeführt werden, um Ihre Strategie zu unterstützen und Domains zu erkennen, die außerhalb dieser Strategie registriert sind. Bei den besten Providern wird diese Analyse praktisch in Echtzeit erfolgen und Sie werden sofort benachrichtigt, wenn mögliche Probleme oder mangelnde Compliance festgestellt werden. Dies bedeutet, dass Sie Ihre Mitarbeiter entsprechend schulen müssen, sobald sie eine Strategie festgelegt haben, der sie folgen sollen.

Mehr darüber unter Punkt 4.

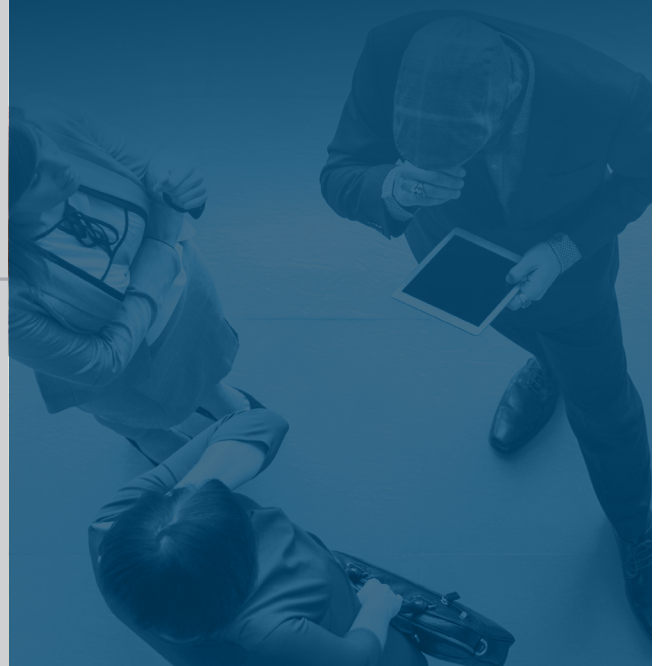
1

2

3

4

Die Auswirkungen eines Vorfalls für Ihr Unternehmen erfassen und entsprechend planen.



Dies ermöglicht Ihnen, sich bei einem Problem noch einmal anzusehen, was geschehen ist, und dies mit der Frage der Business Continuity zu verbinden. Dadurch wird es zum Tagesordnungspunkt einer Vorstandssitzung, was extrem wichtig ist.

Das Business Continuity Institute hat in seinem jährlichen **BCI Horizon Scan Report** von 2018 die 10 wichtigsten Risiken für die Business Continuity festgestellt, die von den 657 Umfrageteilnehmern aus 76 Ländern berichtet wurden. Für viele ist dabei vielleicht überraschend, dass bei vier dieser Risiken digitale Assets ein wichtiger Faktor sind:

- **Cyber-Angriffe.** Das DNS kann einer ganzen Reihe von Cyber-Angriffen ausgesetzt sein, von DNS-Cache-Poisoning, DNS-Hijacking und Domain-Shadowing über Malware und DNS-Tunneling bis hin zu DDoS (Distributed Denial of Service) und Phishing-Angriffe sowie die Nutzung ausgelaufener digitaler Zertifikate.
- **Datenschutzverletzungen.** Cyber-Angriffe auf digitale Assets werden zunehmend dazu genutzt, Daten zu stehlen, entweder indem ein anderer Angriffsvektor verdeckt wird oder indem mangelnde Sicherheit und schlechte Verwaltung von Assets direkt ausgenutzt werden.
- **Ungeplante IT- und Telekommunikationsausfälle.** Wenn Domains oder das DNS eines Unternehmens ausfallen, dann können auch alle Kommunikationsmöglichkeiten über das Internet ausfallen. Wie kann ein Unternehmen aber noch mit Kunden und Mitarbeitern kommunizieren, wenn dies geschieht?
- **Störung der Lieferkette.** Wie kann ein Unternehmen den Geschäftsbetrieb und die Lieferkette aufrecht erhalten, wenn es aufgrund eines Ausfalls von Domains und DNS nicht mehr kommunizieren kann?

Es ist also klar, dass die Auswirkungen gravierend sind und daher unbedingt grundlegende Sicherheitsmaßnahmen für Ihre digitalen Assets ergriffen werden müssen. Die Schwere von Cyber-Angriffen nimmt weltweit zu, und es spielt keine Rolle, ob Sie von politisch engagierten Hackern (Hacktivisten) oder Cyber-Kriminellen angegriffen werden. Fakt ist, wenn es passiert, wird es teuer für das Unternehmen.

Stellen Sie sich folgende Fragen:

- Sind der Zugriff auf und die Berechtigungen für alle Ihre digitalen Assets sicher?
- Welchen Schutz vor DDoS-Attacken nutzt Ihr Unternehmen?
- Welche Lösung verwendet Ihr Unternehmen gegen Phishing oder E-Mail-Betrug?
- Garantiert Ihr DNS-Provider 100 % Uptime?
- Kann er glaubwürdig nachweisen, dass er dies seinen Kunden auch in der Vergangenheit garantiert hat?
- Setzen Sie für Ihre geschäftskritischen Domains alle verfügbaren Sicherheitsmaßnahmen ein, die Ihrem Unternehmen und den Risiken, vor denen Sie stehen, entsprechen?

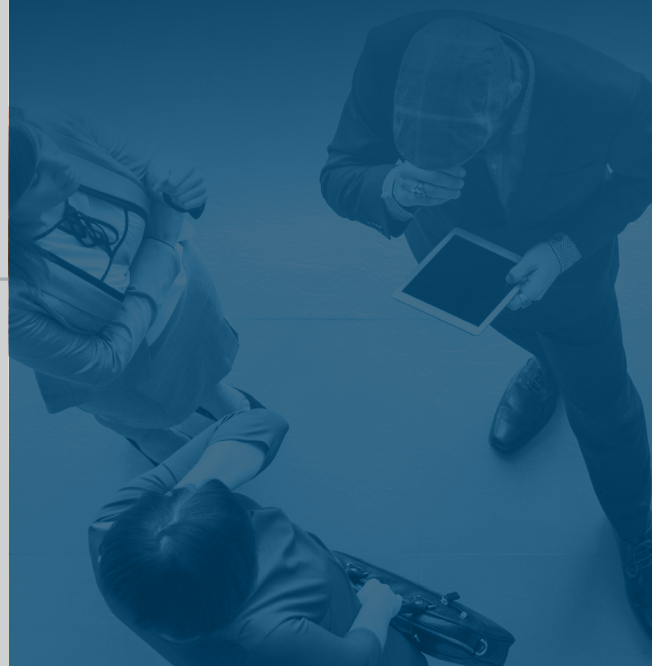
1

2

3

4

Die Auswirkungen eines Vorfalls für Ihr Unternehmen erfassen und entsprechend planen.



Verstehen, welche Assets geschäftskritisch sind.

Eine wesentliche Voraussetzung ist zu verstehen, welche Ihrer digitalen Assets geschäftskritisch sind. Das klingt so einfach, Sie müssen aber erst verstehen, wie Domains von den verschiedenen Funktionen im Unternehmen weltweit genutzt werden.

Wir empfehlen Ihnen, sich mit einem Provider zusammenzutun, der mit einem eingebauten Algorithmus oder über maschinelles Lernen nahezu in Echtzeit Ihre geschäftskritischen Domains identifizieren kann.

Verfolgen Sie den Ansatz Defense in Depth.

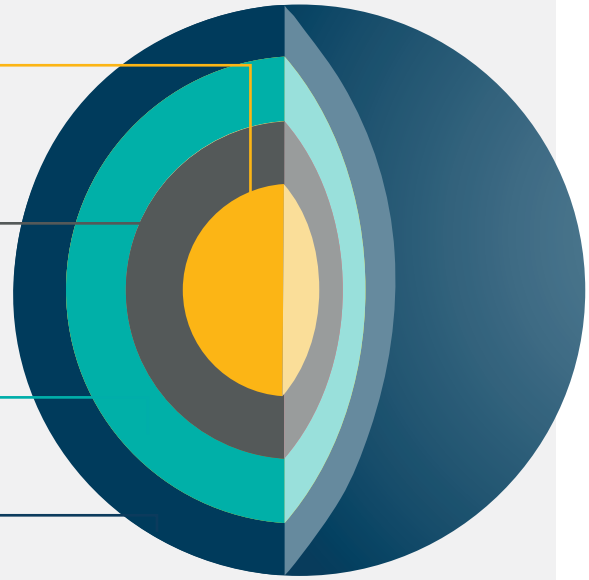
Unter Defense in Depth versteht man den Einsatz mehrerer Sicherheitsmaßnahmen, um die digitalen Assets des Unternehmens gegen die vielen Bedrohungen zu verteidigen, die zu den oben beschriebenen Risiken für die Business Continuity führen können.

EINSATZ HOCHENTWICKELTER SICHERHEITSMERKMALE FÜR IHRE GESCHÄFTSKRITISCHEN DOMAINS
MultiLock, DNSSEC, HTTPS, DMARC und CAA Records

KONTROLLE DER NUTZERBERECHTIGUNGEN
Sichtbarkeit höherer Berechtigungen und Benachrichtigungen

SICHERUNG DES PORTALZUGRIFFS
IP-Validierung, Zwei-Faktor-Authentifizierung und Federated ID

ENTERPRISE-CLASS-PROVIDER
Systeme, Mitarbeiter, Strategien und Prozesse



1

2

3

4

Den ROI optimieren. Wissen, was wichtig ist (zum Beispiel wesentliche Domains) und was nicht.

Zunächst ist festzustellen, dass die meisten aufgeblähte Portfolios mit schlechtem ROI haben, da digitale Assets – insbesondere Domains – relativ kostengünstig erworben werden können. Es ist aber möglich, den ROI nachzuweisen. Dies ist besonders wichtig, da Unternehmen immer mehr für hochentwickelte Sicherheitsmerkmale für die notwendigen Domains ausgeben müssen. Das Konzept ist einfach: Assets, die für Ihre Marke nicht wichtig sind, können Sie auslaufen lassen oder kündigen, um so Mittel für zusätzliche Sicherheitsinvestitionen freizusetzen.

Sie sollten auch dafür sorgen, dass Ihre digital IP zu relevanten Inhalten führt. Dann können Sie den Besucherverkehr messen – ein wichtiger Indikator für den ROI. Vielleicht haben Sie ja immer noch Domains von speziellen Kampagnen, die nicht mehr aktiv sind oder zu einer Hauptdomain umgeleitet wurden. Sie sollten sich ferner auch die Domains ansehen, die aus Abwehrgründen registriert wurden. Sie generieren Falscher Umbruch: "Besucherverkehr" muss mit auf die linke Zeile, verteidigen Ihre Marke aber vielleicht gegen Schutzrechtsverletzungen. Behalten Sie solche Abwehrregistrierungen, wenn sie notwendig sind, und stoßen Sie unnötige Domains wo immer möglich ab, um Ihr Portfolio zu optimieren. Dadurch erhalten Sie Raum, um Lücken bezüglich verfügbarer Domains, einschließlich Marken, zu identifizieren und sie gegebenenfalls zu registrieren.

Allerdings kann ein aufgegebener Domainname eines Unternehmens einen Footprint von Aktivitäten mitführen, der dann als Angriffsvektor genutzt werden könnte. Leerzeile löschen. Falscher Umbruch. Zusammen mit einem Enterprise-Class-Provider sorgfältig überlegt werden. Ein solcher Provider hat die Tools, um notwendige Domains zu identifizieren, und kann somit sicherstellen, dass nur Domains abgestoßen werden, die keinen echten Wert für Sie haben.

1

2

3

4

Die vielen digitalen Kanäle verteidigen.

Wenn Sie dann Ihre digitalen Assets unter Kontrolle haben, sollten Sie sich die Assets ansehen, die Dritten gehören, die Ihre Marke für sich nutzen oder vielleicht sogar vorgeben, Sie zu sein.

Online-Überwachungsservices sind ein wichtiges Asset in den meisten Branchen. Der Grad, in dem Sie Überwachung einsetzen, hängt von Ihrer eigenen digitalen Markenstrategie ab, und auch in dieser Hinsicht sollten Sie sich mit der Rechts- und Marketingabteilung in Verbindung setzen, um herauszufinden, was wichtig und eine Überwachung wert ist und worüber Sie sich keine Sorgen machen müssen.

Bedenken Sie, dass Sie in erster Linie die Sicherheitsrisiken eindämmen möchten, die Rechts- und Marketingabteilung aber verhindern muss, dass Ihre Markenrechte verletzt werden. Trotz dieser unterschiedlichen Motive haben Sie aber ein gemeinsames Ziel – Ihr Unternehmen zu schützen!

Wenn Ihre digitalen Markenüberwachungsaktivitäten auf Ihren Prioritäten basieren, sind sie kosteneffektiver und die größten Bedrohungen werden mit höherer Wahrscheinlichkeit gefunden. Sie werden die „Bösewichte“ identifizieren können, bevor diese in Falscher Umbruch. Eigentums gelangen. Nachdem Sie die richtige Überwachungslösung für Ihre Marke installiert haben, können Sie bestimmen, welche Warnmeldungen am kritischsten sind und ein sofortiges Eingreifen erfordern und möglicherweise diejenigen ignorieren, die Ihre Marke nicht beeinträchtigen. Bedenken Sie aber, dass das Filtern der Überwachungsergebnisse eine andauernde Aufgabe ist.

Durch Überwachung werden Sie auch in der Lage sein, Ihre Sicherheitsstrategien und -kontrollen im Auge zu behalten. Das beginnt schon damit sicherzustellen, dass alle Mitarbeiter Domains nur über Ihren zentral beauftragten Managementpartner registrieren. Ferner ist es wichtig, sich die dazugehörigen DNS und digitalen Zertifikate (SSLs) anzusehen, um zu bestimmen, ob die Domain notwendig ist und ob die richtigen Sicherheitsmaßnahmen auf Basis der Bedeutung der Domains für Ihre Marke eingesetzt werden.

Ein guter Anbieter für Markenüberwachung kann Ihnen bei der Verwaltung der permanenten Barriere helfen; und ein ausgezeichneter Anbieter geht für Sie sogar die Warnmeldungen durch und teilt Ihnen nur die kritischsten Verstöße mit, die Ihre Aufmerksamkeit erfordern.

CSC Security Center

CSC Security Center℠ erfüllt ein bisher unerfülltes Bedürfnis der Branche – die vollständige Kontrolle über die wichtigsten Domains einer Marke. Die einzigartige Lösung wurde mit den modernen firmeneigenen Algorithmen von CSC mit dem Ziel entwickelt, die umfassendste Domain-Namen-Sicherheitslösung auf dem Markt bereitzustellen. Sie identifiziert notwendige Domains, überwacht das System auf Bedrohungen, verschickt Benachrichtigungen, wenn Veränderungen festgestellt werden, und erleichtert das Eindämmen von Sicherheitsbedrohungen. Informieren Sie sich über das CSC Security Center und wie es die Art Ihrer Verwaltung der digitalen Assets verändert und gleichzeitig die Cyberrisiken verringert.

cscdigitalbrand.services/de

CSC ist ein Service-Unternehmen und bietet keine Finanzberatung an. Die hier veröffentlichten Materialien dienen nur zu Informationszwecken. Bitte wenden Sie sich an Ihren Rechts- oder Finanzberater, um herauszufinden, inwiefern diese Informationen auf Sie zutreffen.