WENN PERSONEN DIE ROLLEN WECHSELN—

Best Practices für Digitale Vermögenswerte

cscdbs.com/de

i EINLEITUNG

1 ÜBERPRÜFEN

2 ERSETZEN

3 DEAKTIVIEREN

4 BEST PRACTICES

EINLEITUNG

Bei der Verwaltung der Digitalen Vermögenswerte eines Unternehmens, wie z. B. Domains, Domain Name Systeme (DNS) und digitale Zertifikate, müssen alle Administratoren einen Aspekt besonders im Blick behalten: Welche Personen haben Zugriff auf das Portfolio und wo sind deren personenbezogene Daten aufgeführt? Angesichts zunehmender Sicherheitsvorfälle und strengerer Datenschutzgesetze ist es wichtiger denn je, den Überblick über die verwendeten Anmeldeinformationen und personenbezogenen Daten der Benutzer zu behalten und sicherzustellen, dass die Daten regelmäßig aktualisiert werden, um Sicherheits- und Compliance-Risiken zu vermeiden.

Wenn Mitarbeiter ein Unternehmen verlassen oder die Rolle wechseln, empfiehlt CSC, alle Anbieterportale, Domainnamen und andere Vermögenswerte zu überprüfen, um sicherzustellen, dass die Benutzerdaten sofort in allen Produkten und Diensten aktualisiert werden.

ÜBERPRÜFEN

Wir empfehlen eine regelmäßige Überprüfung der Benutzer und der Zugriffsrechte für alle Anbieterportale. Schon aufgrund der Unvermeidbarkeit menschlicher Fehler sind Menschen das schwächste Glied in jeder Organisation, und gute Richtlinien für die Benutzerverwaltung sind entscheidend, um ein hohes Maß an Sicherheit zu erhalten.

Überprüfen Sie Ihre Benutzer regelmäßig (mindestens alle 90 Tage).
CSC Security CenterSM kann Ihnen helfen, Aktualisierungen für alle autorisierten Benutzer einfach anzuzeigen und anzufordern und auch Benachrichtigungen einzurichten, wenn neue Benutzer hinzugefügt werden.

Überprüfen Sie Ihre Daten im WHOIS-Portfolio mindestens einmal im Jahr.
Gemäß der WHOIS Data Reminder Policy (WDRP) sollten Sie sicherstellen, dass Ihre WHOIS-Daten aktuell und korrekt sind.

Überprüfen Sie Ihre Konten in sozialen Medien.

Denken Sie an die Löschung der Benutzerdaten.
Das „Recht auf Vergessenwerden“ – auch bekannt als „Recht auf Löschung“ – gewährt EU-Bürgern das Recht, die Löschung ihrer Daten zu verlangen. Es wird empfohlen, dass beim Ausscheiden eines Benutzers seine personenbezogenen Daten aus dem Public-WHOIS entfernt werden, sowohl wegen der Sicherheitsrisiken als auch aufgrund von Vorschriften zum Schutz der Privatsphäre und des Datenschutzes. CSC kann Sie bei der Prüfung aller Tools und Dienste, auf die der Mitarbeiter Zugriff hatte, unterstützen und das Risiko durch die vollständige Entfernung nicht mehr gültiger Kontakte reduzieren.

2

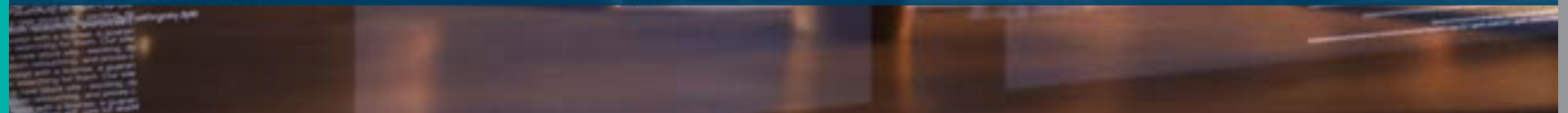
ERSETZEN

In jeder Organisation werden Benutzern oft mehrere Aufgaben zugeordnet, die über den normalen Zugriff auf das Benutzerportal hinausgehen. Es ist wichtig, eine Bestandsaufnahme der zusätzlichen Funktionen zu machen, die eine Person ausgeführt hat, und sicherzustellen, dass ein geeigneter Ersatz gefunden wird.

Welche Funktionen hat der Mitarbeiter ausgeführt:

- Kontaktperson für Erneuerungen?
- Kontaktperson für besondere Benachrichtigungen?
- Kontaktperson in den WHOIS-Kontaktangaben für eine Domain?
- Empfang und Bearbeitung von Rechnungen für das Unternehmen?
- Funktionen in Verbindung mit Sicherheitsdiensten?

Nachdem alle diese Bereiche identifiziert wurden, können Sie leicht bestimmen, wer diese Kontaktperson ersetzen soll, und die Zugangsinformationen entsprechend aktualisieren.



3

DEAKTIVIEREN

Als erster Schritt ist es wichtig, dass die Benutzeranmeldeinformationen rechtzeitig deaktiviert werden. Mit Single Sign-On oder förderierter ID haben Sie direkte Kontrolle über die Benutzeranmeldeinformationen und können die Anmeldedaten eines Benutzers schnell deaktivieren.

- CSCDomainManager℠
- CSC Security Center
- Markenschutzportale
- Portale für das DNS und digitale Zertifikate

Außerdem ist es wichtig, alle Tools von Drittanbietern zu verfolgen, auf die der Mitarbeiter Zugriff hatte, und sicherzustellen, dass die Zugriffsrechte entsprechend aktualisiert werden.

Teilen Sie Ihren Anbieterpartnern alle organisatorischen Änderungen mit. CSC prüft gerne die bestehenden Zugriffsrechte und stellt sicher, dass Aktualisierungen zeitnah und auf allen verfügbaren Plattformen durchgeführt werden.
Wir helfen Ihnen gerne.

4

BEST PRACTICES

- Beschränken Sie den Zugriff auf Anbieterkonten auf die notwendigen Benutzer. Stellen Sie sicher, dass Anbieterportale die Implementierung zusätzlicher Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung und IP-Validierung ermöglichen.
- Ziehen Sie Single Sign-On in Betracht, um die Anmeldedaten der Benutzer zu kontrollieren.
- Konsolidieren Sie Anbieter, wenn es möglich ist. Weniger Portale und Anbieterkonten bedeuten auch weniger zu verwaltende Anmeldedaten.
- Überprüfen Sie Ihre Benutzer regelmäßig (mindestens alle 90 Tage). CSC Security CenterSM kann Ihnen helfen, Aktualisierungen für alle autorisierten Benutzer einfach anzuzeigen und anzufordern und auch Benachrichtigungen einzurichten, wenn neue Benutzer hinzugefügt werden.
- Stellen Sie sicher, dass Sie für alle Kontaktpersonen geeigneten Ersatz haben, bevor Sie sie in Ihren Anbieterportalen deaktivieren.

cscdbs.com/de @cscdbs CSC Digital Brand Services

DBS03302021