digitale vermögenswerte SICHERHEITS-CHECKLISTE

DIGITALE VERMÖGENSWERTE
Anbietermanagement

- ☐ Sie haben eine KOMPLETTE Übersicht all Ihre Domains, Domainnamensysteme (DNS) und SSL (Secure Sockets Layer)-Anbieter.
- ☐ Alle Anbieter Ihrer digitalen Vermögenswerte bieten Vollzeitsupport auf Unternehmensebene, 24/7/365.
- ☐ Alle Anbieter Ihrer digitalen Vermögenswerte haben stark in den Schutz ihrer Systeme investiert, z.B. in Datencenter nach ISO 27001, SOC 2®-konforme Tests auf Eindringen von Dritten, Schwachstellen- und Sicherheitstests, darunter SQL-Einschleusung und XSS etc.
- ☐ Alle Anbieter Ihrer digitalen Vermögenswerte haben stark in die Schulung ihrer Mitarbeiter investiert, z.B. in Sicherheitstraining, Sensibilisierung für Phishing durch regelmäßige Phishing-Testmails, Zwei-Faktor-Authentifizierung für den Fernzugang etc.
- ☐ Alle Anbieter Ihrer digitalen Vermögenswerte haben stark in den Schutz ihrer Kunden investiert, z.B. in IP-Validation, Zwei-Faktor-Authentifizierung, autorisierte Kontaktpersonen, die Übermittlung von Aufträgen erfolgt immer schriftlich und niemals telefonisch, föderierte Identität etc.
- ☐ Keiner Ihrer Anbieter ist in der Vergangenheit auf Phishing, Social Engineering, DNS-Hijacking oder DDoS (Distributed Denial of Service)-Attacken hereingefallen.
- ☐ Alle Anbieter Ihrer digitalen Vermögenswerte nutzen vorrangig ihre eigenen Zulassungen, statt sich ausschließlich auf Dritte zu verlassen. Ihr Domainanbieter benutzt z.B. bei den Registrys vorrangig seine eigenen Zulassungen, und Ihr Zertifikatsanbieter ist selbst eine akkreditierte Zertifizierungsstelle.

DOMAIN
Management

- ☐ Sie haben eine KOMPLETTE Übersicht Ihres gesamten Domainnamenportfolios.
- ☐ Sie haben mit Ihren Anbietern automatische Verlängerungen vereinbart, unterstützt durch Kontoguthaben.
- ☐ Alle Mitarbeiter sind geschult in einem zentralisierten Ablauf zur Registrierung neuer Domains, und befolgen ihn auch.
- ☐ Es gibt klare Richtlinien zur WHOIS-Vorlage und zu nutzerdefinierten Feldern, die bei der Registrierung vorliegen müssen.
- ☐ Sie nutzen ein Verfahren zur Identifizierung von Unternehmensregistrierungen, die außerhalb der zentralen Richtlinie liegen.

DNS
Management

- ☐ Sie haben eine KOMPLETTE Übersicht Ihres gesamten DNS-Anbieter-Portfolios.
- ☐ Sie nutzen ein Verfahren zur Identifizierung von Domains, die sich nicht auf Unternehmens-DNS mit garantiert hundertprozentiger Betriebszeit befinden.
- ☐ Alle Mitarbeiter sind darin geschult, alle neuen, wichtigen Domains auf Unternehmens-DNS zu legen, und halten sich auch daran.

SSL
Management

- ☐ Sie haben eine KOMPLETTE Übersicht Ihrer SSL-Anbieter.
- ☐ Alle Mitarbeiter sind geschult in einem zentralisierten Ablauf zum Kauf neuer und Ersetzen alter Zertifikate, und befolgen ihn auch.
- ☐ Sie nutzen ein Verfahren zur Identifizierung von SSL-Zertifikaten, die außerhalb Ihrer zentralen Richtlinie erworben wurden.

WICHTIGE (GESCHÄFTSKRITISCHE) DOMAINS
Management

- ☐ Sie können auf Anhieb alle wichtigen Domains identifizieren und nachweisen, dass sie sicher sind.
- ☐ Alle Anbieter für Ihre wichtigsten Domains garantieren eine hundertprozentige Betriebszeit und können dies auch nachweisen.
- ☐ Alle wichtigen Domains benutzen ein passendes SSL-Zertifikat auf Unternehmensebene.
- ☐ Alle wichtigen Domains benutezn Sicherheitsextensions für Domainnamensysteme, um gegen DNS-Cache-Vergiftung zu schützen.
- ☐ Alle wichtigen Domains benutzen Multilock zum Schutz gegen DNS-Hijacking.
- ☐ Alle wichtigen Domains benutzen E-Mail-Authentifizierungsdienste.

BEDROHUNGSABWEHR
Fortsetzung

- ☐ Sie benutzen zusätzliche DDoS-Abwehrdienste, um andere Server jenseits des DNS zu schützen.
- ☐ Sie kombinieren E-Mail-Authentifizierungsdienste mit Phishing-Überwachung und Takedown-Diensten, um die Gefahr von Phishing-Angriffen zu minimieren.

+49 (0)6122 707720 cscdigitalbrand.services/de