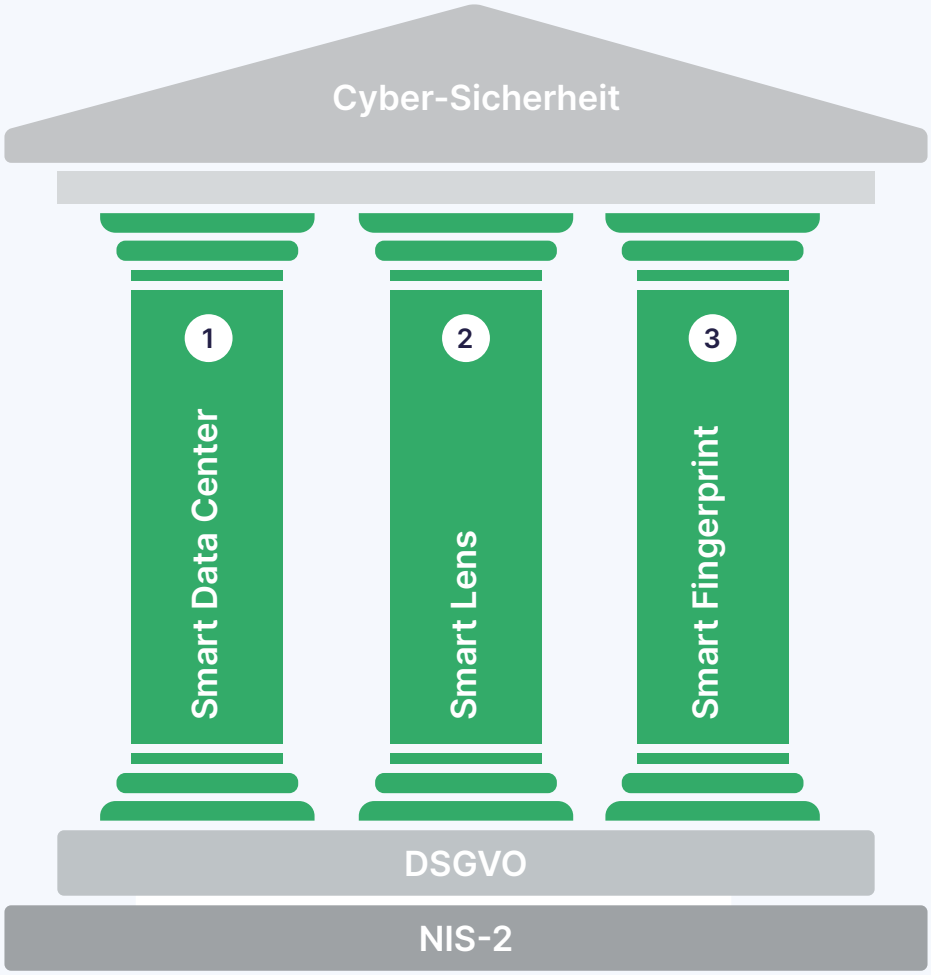
Die drei Säulen Ihrer Cybersecurity-Strategie.

Smart DataCenter

Die Grundpfeiler der Cyber-sicherheit im Überblick!

Cybersecurity ist ein Begriff, der häufig diskutiert wird. Doch anstatt sich darauf zu konzentrieren, was Cybersecurity ist, sollten wir uns bewusst machen, was sie nicht ist: verzichtbar. In der digitalen Welt sind angemessene Sicherheitsvorkehrungen essenziell, da Unternehmen sonst ihre Daten, ihren Ruf und ihre Existenz riskieren.

Unsere Lösungen bieten Ihrem Unternehmen höchste Sicherheit, nahtlos integriert in Ihre IT-Infrastruktur, um umfassenden Schutz vor täglichen digitalen Bedrohungen zu gewährleisten. Durch unsere Lösungen stellen wir sicher, dass Ihr Unternehmen jederzeit vor den neuesten Cyber-Bedrohungen geschützt ist. Cybersecurity ist nicht nur eine technische Herausforderung, sondern auch eine strategische Notwendigkeit. Schützen Sie Ihre Geschäftsabläufe und Ihre Unternehmenswerte mit unserer umfassenden Cybersecurity-Strategie.



Säule 1

Vollautomatisiertes und digitalisiertes Rechenzentrum – Smart Data Center GmbH.

Wir bieten wir Ihnen ein voll automatisiertes und vollständig digitalisiertes Rechenzentrum zur Nutzung an. Das entscheidende Merkmal ist der vollständig automatisierte Prozess für Back-ups – inklusive einer umfassenden Back-up-Strategie (Disaster-Recovery-Test), die Ihnen den kompletten Test Ihres eigenen Back-ups ermöglicht.

Dank dieser Technologie haben Sie die Sicherheit, dass Sie im Fall eines erfolgreichen Hackerangriffs Ihre Daten geschützt bleiben und Sie ohne Zahlung eines Lösegeldes wieder sicher auf die Beine kommen.

Unser Service gibt Ihnen die Gewissheit, dass Sie im Ernstfall selbst die von Ihnen persönlich überprüfte Wiederherstellung aller Daten und Systeme gewährleisten können.

Säule 2

Reduzierung der Wahrscheinlichkeit, überhaupt gehackt zu werden – Smart Lens.

Mit Smart Lens können Sie alle gewünschten Angriffsoberflächen, wie z. B. Ihre Website Ihren Onlineshop, Ihre Datenbanken oder Ihr Intranet einmalig hinterlegen und kontinuierlich überwachen lassen. Unsere Software führt automatisierte Überprüfungen durch und erkennt (optional in Echtzeit) potenzielle Bedrohungen in der Minute ihres Entstehens.

Ein benutzerfreundliches Dashboard gibt Ihnen einen klaren Überblick über die aktuelle Bedrohungslage. Bei allen neuen und vorhandenen Sicherheitslücken erhalten Sie automatisch detaillierte Berichte per E-Mail, sodass Sie sofort reagieren können.

Unsere Lösung stellt sicher, dass Sie für jede Angriffsoberfläche klare und leicht verständliche Berichte erhalten. Darüber hinaus wird ein Risiko-Score von 1 – 10 ausgegeben, der die Bewertung nach Schweregrad, Schadenshöhe und Ausnutzbarkeit der analysierten Sicherheitsrisiken anhand der internationalen CVSS-Werte (Common Vulnerability Scoring System) ermöglicht. Mit diesen Funktionen können Sie die Sicherheitslage Ihres Unternehmens als Geschäftsführer transparent, präzise sowie objektiv einschätzen und gezielt die richtigen Maßnahmen ergreifen.

Säule 3

Absicherung durch einen weiteren biometrischen Faktor – Smart Fingerprint.

Dank unserer Software „Smart Fingerprint“ (verfügbar voraussichtlich ab 10/2024) führen Sie in Ihrem Unternehmen einen weiteren biometrischen Faktor ein. Mit unserer KI überwachen Sie die Nutzung der Internetbrowser und entdecken auf diese Weise erfolgreich eingedrungene Hacker bevor diese zuschlagen können.

Wie funktioniert das? Wenn ein bösartiger Hacker trotz aller Vorsichtsmaßnahmen beispielsweise in den Besitz des Administrator-Passworts gelangt und versucht, kritische Befehle wie „Alles löschen“, „Alles verschlüsseln“ oder „Gib mir ein neues Super-Admin-Passwort“ einzugeben, erkennt die KI anhand der Nutzung des Browsers, der Tastatur und der Maus, dass der Zugriff nicht durch den rechtmäßigen Nutzer, sondern durch einen Hacker erfolgt. Die Art und Weise, wie wir surfen, ist ein absolut eindeutiges biometrisches Merkmal. Die Smart Cyber Security GmbH hat dies als internationales Unternehmen erkannt und dafür eine hochintelligente KI-Software entwickelt. Sogar im Fall eines bereits eingedrungenen Hackers kann diesem live und in Echtzeit das Handwerk gelegt werden.

Sobald eine unberechtigte Nutzung vermutet wird, entzieht die KI diesem Account unmittelbar sämtliche Rechte. Parallel fordert sie – sofern von Ihnen gewünscht und konfiguriert – über eine Zwei-Faktor-Authentifizierung eine Freigabe per SMS an. Diese Freigabeaufforderung richtet sich sowohl an den rechtmäßigen Nutzer als auch an einen Dritten (zum Beispiel Ihren IT-Chef oder an den Geschäftsführer). Solange beide Freigaben nicht erfolgt sind, bleiben die Nutzungsrechte entzogen und der Hacker-Angriff wird effektiv wirkungslos.

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

+49 40 741 24 16 0
kontakt@smart-datacenter.de
www.smart-datacenter.de

Smart DataCenter