



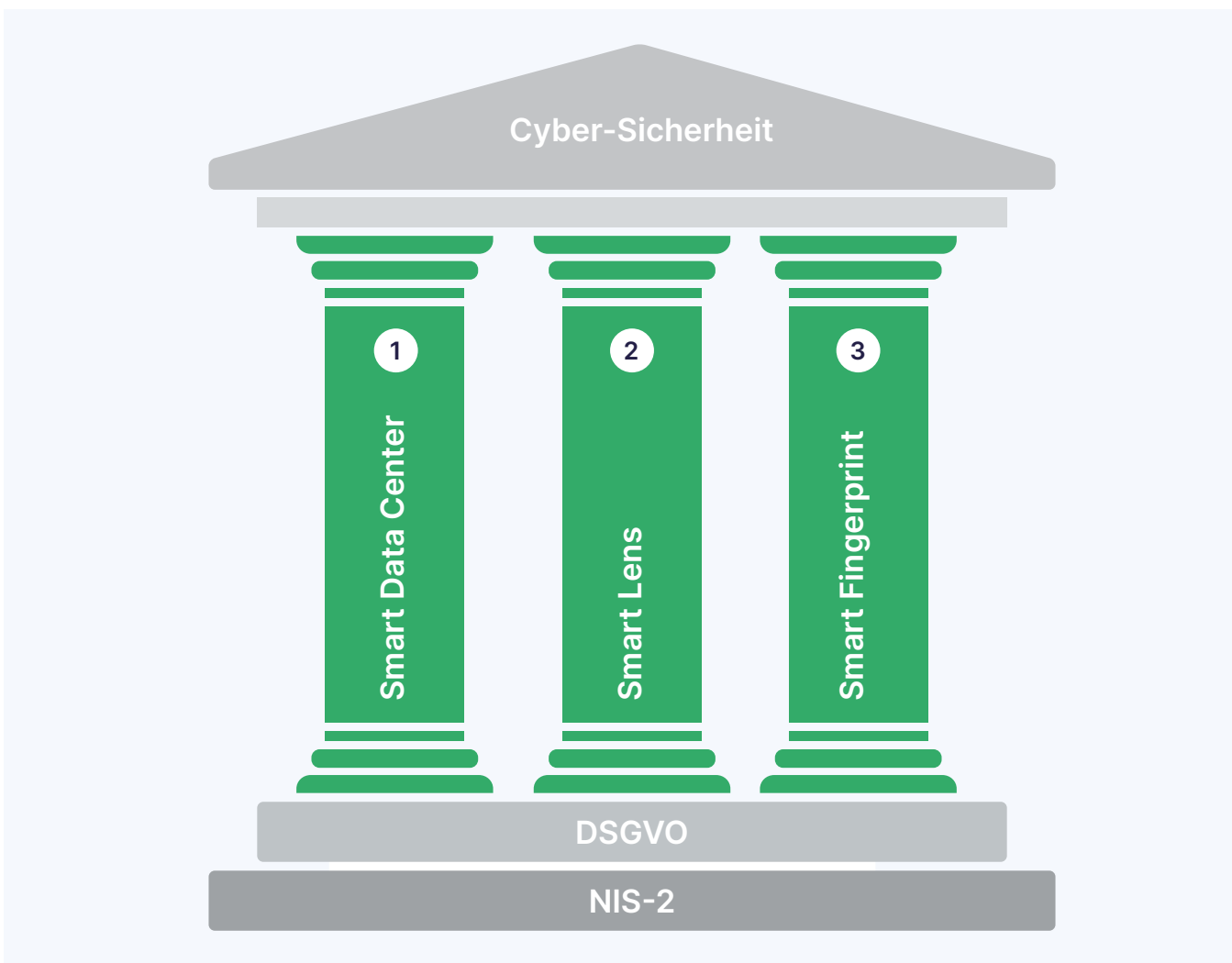
# Die drei Säulen Ihrer Cybersecurity-Strategie.



# 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.



# Vollautomatisiertes und digitalisiertes Rechenzentrum – Smart Data Center GmbH.



Mit dem Smart Data Center bieten wir das weltweit erste vollautomatisierte und vollständig digitalisierte Rechenzentrum an. Das alles entscheidende Alleinstellungsmerkmal dieses Produkts ist der vollständig automatisierte Prozess für Backups inklusive eine umfassende Backup-Strategie (Disaster-Recovery-Test), welche Ihnen erstmals den kompletten Test Ihres eigenen Backups ermöglicht.

Nur dank dieser Technologie, die ohne ein vollständig automatisiertes Rechenzentrum allein technisch nicht verfügbar wäre, haben Sie die Sicherheit, dass Sie im schlimmsten Fall eines erfolgreichen Hackerangriffs trotz aller Sicherheitsmaßnahmen zu 100% sicher und ohne Zahlung eines Lösegeldes wieder auf die Beine kommen.

Da niemand – auch trotz der unter Säule eins und zwei genannten Maßnahmen – jemals 100% Sicherheit vor einem erfolgreichen Angriff erlangen kann, kommt der durch sie selbst persönlich überprüften Wiederherstellung aller Daten und Systeme in der heutigen Welt neuerdings die allergrößte Bedeutung zu.

# 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 und objektiv einschätzen und gezielt die richtigen Maßnahmen ergreifen.



# Absicherung durch einen dritten „biometrischen Faktor“ – Smart Fingerprint.



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

Wie funktioniert das? Wenn ein böstiger Hacker trotz aller Vorsichtsmaßnahmen beispielsweise in den Besitz des Administrator-Passworts gelangt und versucht, kritische Befehle wie „Alles löschen“, „Alles verschlüsseln“ oder „Gebe 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 ist das erste internationale Unternehmen, das diesen Umstand erkannt und in eine hochintelligente KI-Software umgesetzt hat. So können wir Ihnen sogar im Falle eines bereits eingedrungenen Hackers diesem live und in Echtzeit das Handwerk legen.

Sobald eine unberechtigte Nutzung vermutet wird, entzieht die KI auf der Stelle zunächst sämtliche Rechte dieses Accounts und fordert – sofern von Ihnen gewünscht und konfiguriert – sogar über eine Zwei-Faktor-Authentifizierung sowohl beim rechtmäßigen Nutzer als auch bei einem dritten Faktor (zum Beispiel Ihrem IT-Chef oder Geschäftsführer) eine Freigabe per SMS an. Solange beide Freigaben nicht erfolgt sind, bleiben die Nutzungsrechte entzogen und der Hacker-Angriff wird effektiv wirkungslos.