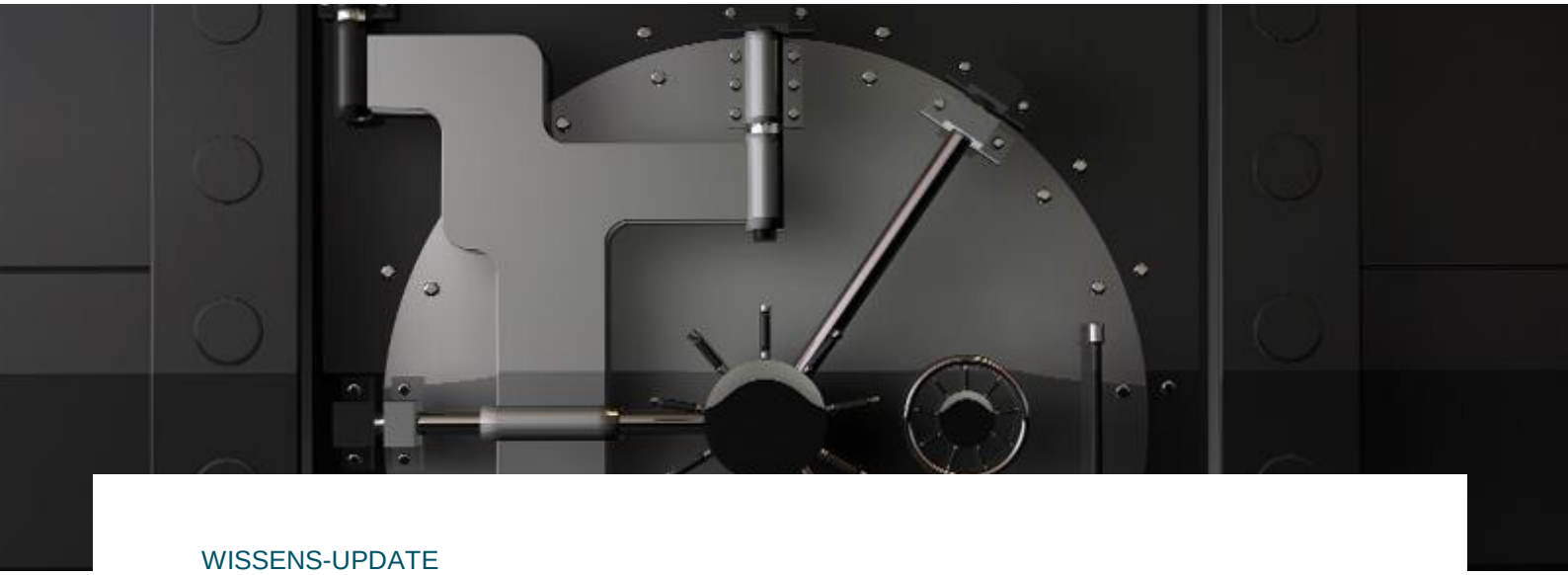
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

«Saved in Switzerland» – auf dem Weg zum internationalen Daten-standort

Politische Stabilität, Rechtssicherheit, Neutralität, Qualität – die Schweiz hat beste Chancen, der sichere Datentresor der Welt zu werden. Um die Digitalisierung auf diese Weise ökonomisch gewinnbringend zu nutzen, muss die Schweiz allerdings eines werden: cybersouverän. Dafür braucht sie eine starke IT-Sicherheitsarchitektur. Unter anderem.

Digitale Eigenständigkeit: Was auf den ersten Blick wie ein vollendeter Widerspruch erscheinen könnte, ist tatsächlich das Gegenteil. Denn Souveränität im Internet bedeutet nicht, dass sich die Schweiz digital abschotten soll; da wäre unser Land als kleine Exportnation mehr als schlecht beraten. Es geht genau umgekehrt um internationale Zusammenarbeit. «Wenn der Handlungs-spielraum auf nationaler Ebene kleiner wird, ist ein stärkeres und wirksameres Einbringen auf internationaler Ebene gefordert, damit die Spielregeln des globalen digitalen Raumes nach den eigenen Werten, Prinzipien und Interessen mitgestaltet werden können», formulierten es Philipp Metzger und Thomas Schneider vom Bundesamt für Kommunikation in der Zeitschrift für Datenrecht und Informationssicherheit Digma vor einigen Jahren sehr treffend.

Verstärkte Kooperation mit der Industrie

Doch als digitaler Player auf internationaler Ebene hat die Schweiz noch viel mehr Potenzial, als sich selber wirksam vor Cyber-Risiken zu schützen: das Potenzial, sich die Digitalisierung ökonomisch gewinnbringend zunutze zu machen. Oder konkreter: *der* sichere Datentresor auch für ausländische Unternehmen und Regierungen zu werden.

Bereits heute besetzt die Schweiz im Ranking des Data-Centre-Risk-Indexes, das die Länder weltweit nach Attraktivität für Daten- und Rechenzentren auflistet, den dritten Platz. «Saved in Switzerland» – Faktoren wie politische Stabilität und Rechtssicherheit, aber auch kulturelle Merkmale wie Zuverlässigkeit, Neutralität und Qualität wirken offenbar anziehend auf ausländische Unternehmen. Hinzu kommt die starke Schweizer Industrie mit ihrem enormen technischen Innovationspotenzial. Um darauf zugreifen und diese Karte spielen zu können, ist jedoch eine intensivere und vor allem koordinierte Zusammenarbeit mit diesem Sektor nötig.

Resilienz durch eine starke Sicherheitsarchitektur und Security by Design

Damit sich die Schweiz aktiv als sicheren Standort für Daten, Cloud-Dienste und IT-Provider aus aller Welt etablieren kann, sind auch angemessene datenschutzrechtliche Rahmenbedingungen gefragt. Der staatliche, garantierte Schutz der Privatsphäre ist dabei zentral. Dazu benötigen Bund, Kantone und Gemeinden eine gemeinsame Vision und Strategie für einen sicheren Cyber-Raum, welche in einheitlichen international anerkannten hohen Standards münden.

Die Bundesverwaltung muss jetzt den Lead übernehmen, damit unser Land auch künftig selbstbestimmt agieren kann. Zumal Staaten ihre militärischen Interessen ebenfalls zunehmend online verfolgen – bis hin zum virtuellen Wettrüsten. Zusätzlich nimmt die Wahrscheinlichkeit von Cyber-Terrorismus mit dem technologischen Fortschritt zu. Digitalisierte Systeme und Prozesse bieten eine höhere Angriffsfläche.

Konkret gibt es folgende **Handlungsfelder**, damit die Schweiz souverän mit derartigen Bedrohungen umgehen kann:

- Durch eine komplette oder umfassende und gut abgestimmte Sicherheitsarchitektur Resilienz schaffen: Viren oder Malware schnell und effektiv isolieren.
- Kritische Informationsräume (z. B. Krankenhäuser) definieren und schützen: Kommunikationsbeziehungen entflechten und Übergänge kennen.
- «Security by Design»: Im Voraus planen, wie Prozessoren, Festplatten oder Browser in geschützte und ungeschützte Bereiche abgetrennt werden können; entweder in der Software oder – noch sicherer – in der Hardware.
- Supply Chain Security: Transparente und robuste Wertschöpfungsketten schaffen.

Wissenschaftlich fundierte und trotzdem praxisnahe Bildung

Sehr wohl ist Technologie die Grundlage, um Cybersouveränität herzustellen. Im Zentrum steht allerdings nach wie vor der Mensch. Er ist es, der IT-Sicherheitskonzepte entwirft und Entscheidungen trifft; dafür braucht er die nötigen Kompetenzen, ob auf Behördenseite oder in Unternehmen. Er braucht gute, wissenschaftlich fundierte und trotzdem praxisnahe Bildungsangebote in sämtlichen Feldern und Schichten der Digitalisierung. Und auch hier gilt: Diese Angebote müssen zwingend auf internationale Vernetzung ausgelegt sein, statt sich lediglich auf die Schweiz zu konzentrieren.

CyOne Security ist der vertrauensvolle Partner auf dem Weg zum Datentresor Schweiz

Es gilt also, die Schweiz vor Cyber-Risiken zu schützen indem einheitliche Cyber-Sicherheits-standards für die Schweiz definiert und umgesetzt werden. Diese sollen in einer schweizweiten umfassenden und aufeinander abgestimmten Sicherheitsarchitektur münden. Moderne und effiziente Informations- und Kommunikationstechnologie bildet das Rückgrat von Staat und Wirtschaft und ist unabdingbar auf dem Weg zum sicheren Datentresor. Agil, skalierbar und mit

einer gesicherten Verfügbarkeit trägt sie entscheidend zum nachhaltigen Erfolg eines sicheren Datentresors in der Schweiz bei.

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Cyber-Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Ihre Organisation vor Cyber-Risiken zu schützen und tragen Sie so zur Vision eines sicheren Datentresors in der Schweiz bei.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Cyber-Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.