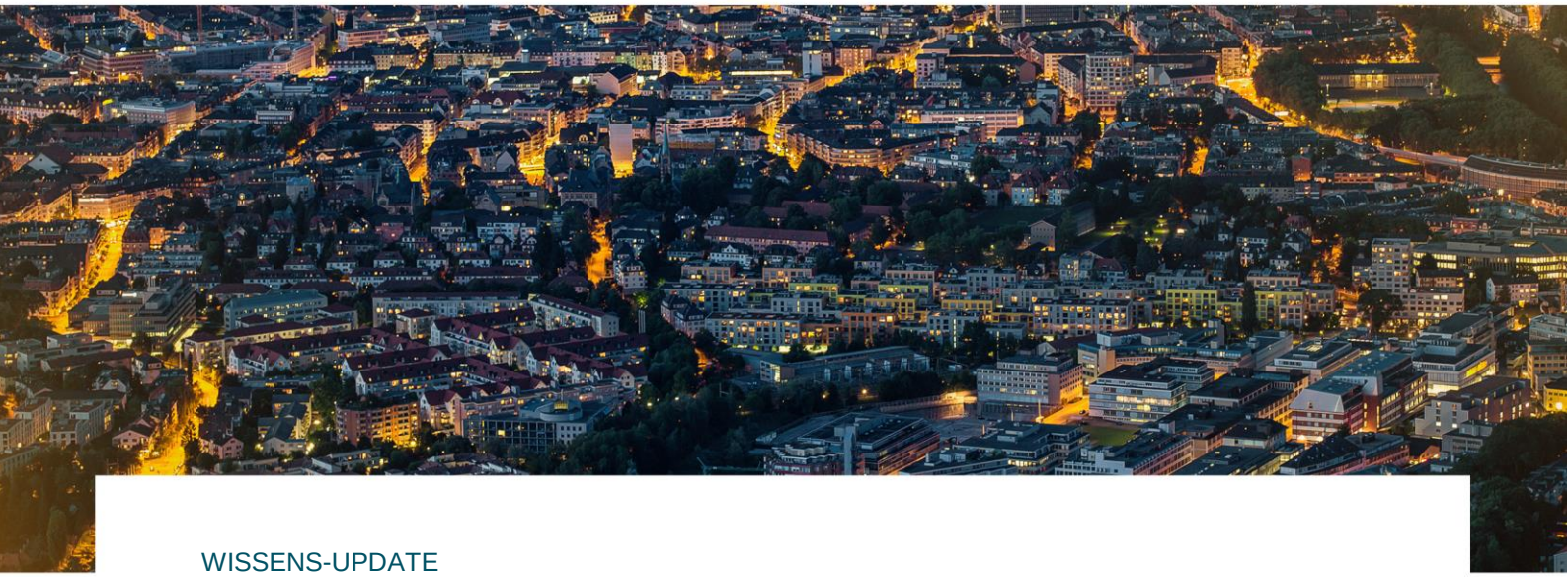
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

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



WISSENS-UPDATE

Cyber Security – nur wenn die gesamte Supply Chain geschützt ist

Fabian Schmid | Senior Security Consultant | Steinhausen, 12. Juli 2022

Die Cyber-Souveränität der Schweiz ist bedroht. Um sie zu wahren, sind Politik und Wirtschaft gleichermassen gefordert. Das Thema Cyber Security muss rasch und konsequent angepackt werden – am besten mit Unterstützung durch Schweizer Spezialisten.

Der Bundesrat ist unter Zugzwang: Er muss das Thema Cyber Security mit aller Konsequenz angehen. Die Zeit drängt, denn die Angriffe auf Schweizer Unternehmen und Institutionen mehren sich. Während das Thema bei den führenden Wirtschaftsmächten schon lange höchste Priorität hat, behandelte es der Bund bisher eher zu stiefmütterlich. Sowohl das Parlament als auch Exponenten aus Wissenschaft und Wirtschaft kritisierten die Regierung in der Vergangenheit für ihre zögerlichen Schritte.

Nun aber macht der Bundesrat Nägel mit Köpfen. Er hat das Nationale Zentrum für Cybersicherheit geschaffen. Dieses bildet eine strategische Einheit im Generalsekretariat des Eidgenössischen Finanzdepartements (EFD) und ist von einem Delegierten des Bundesrats geleitet. Der Vorsitzende des Kompetenzzentrums ist Ansprechpartner für Politik, Medien und Bevölkerung, leitet Gremien im Bereich Cyber-Risiken und arbeitet eng mit der Wirtschaft zusammen.

Sicherheitspolitik unter digitalen Vorzeichen

Die Organisationsstruktur zeigt: Der Bundesrat versteht Cyber Security als Aufgabe der obersten Führungsverantwortung. Es ist denn auch dringend nötig, dass die Regierung eine aktive Rolle übernimmt, um die Bevölkerung und die Wirtschaft beim Schutz vor Cyber-Risiken zu unterstützen. Gleichzeitig muss der Bund die Sicherheit der eigenen IT-Systeme ständig verbessern, um die Cyber-Souveränität der Schweiz zu wahren.

Die digitale Transformation verändert nicht nur Gesellschaft und Wirtschaft, sie sorgt auch für einen Paradigmenwechsel in der Sicherheitspolitik. Für die Regierungen geht es heute längst nicht mehr nur darum, territoriale Ansprüche mit politischen und militärischen Mitteln sicherzustellen. Der kaum überschaubare und weltweit durchlässige Cyberspace stellt die Souveränität der Staaten auf die Probe. Souverän ist heute, wer die digitale Informationshoheit hat, die Sicherheit und die Verfügbarkeit der Datenströme gewährleisten kann.

Grosse Abhängigkeit vom Ausland

Die Schweizer Wirtschaft ist in hohem Masse vom Ausland abhängig. Die starke internationale Vernetzung ist für unsere Volkswirtschaft überlebenswichtig. Im Cyberspace birgt die globale Verflechtung jedoch auch Risiken. Einerseits kennt Cyber Security keine Landesgrenzen – die meisten Cyber-Attacken stammen aus dem Ausland, andererseits ist die Schweiz nicht nur von ausländischen Märkten abhängig, sondern auch von ausländischer Soft- und Hardware. Institutionen und Unternehmen stützen sich mehrheitlich auf Lösungen aus den USA, China, Israel und einigen weiteren Ländern.

Als kleines Land ist die Schweiz auf internationale Kooperationen im Bereich Cyber Security angewiesen, denn im Alleingang lässt sich dieses komplexe Thema nicht bewältigen. Dennoch: Um die Cyber-Souveränität des Landes sicherzustellen, ist es notwendig, dass die Schweiz die Schlüsseltechnologien in der Cyber Security selbst in der Hand hält. Dafür muss der hiesige IT-Sektor zum einen mehr eigenständige Lösungen entwickeln. Dieses Know-how liesse sich dann wiederum gewinnbringend an strategische Partner im Ausland exportieren. Zum anderen müssen Politik und Wirtschaft bei der Gestaltung der IT-Infrastruktur das Kriterium «Swissness» höher gewichten.

Die gesamte Supply Chain schützen

Wie die Bestrebungen des Bundesrats zeigen, hat die Politik die Bedeutung der Cyber-Souveränität für die Schweizer Volkswirtschaft mittlerweile erkannt. Auch in der Wirtschaft wächst das Bewusstsein für die Relevanz des Themas. Unternehmen begreifen allmählich, dass der Bereich Cyber Security grosse Risiken mit sich bringt und in Geschäftsprozessen eine zunehmend erfolgskritischere Rolle spielt, insbesondere im Umfeld von Industrie 4.0. Zudem tragen Organisationen im Bereich Cyber Security eine grosse Verantwortung. Sie haften nämlich nicht nur für die Sicherheit der eigenen IT-Systeme, sondern können auch für einen Cyber-Angriff auf einen Geschäftspartner, mit dem Daten ausgetauscht werden, verantwortlich gemacht werden.

Die zunehmende Vernetzung der IT-Systeme über die gesamte Wertschöpfungskette hinweg erhöht die Anforderungen an die Cyber Security. Denn über das schwächste Glied der Kette können sich Angreifer Zugriff auf das komplette Lieferantennetzwerk verschaffen. Der Begriff des «Supplier Risk Management» muss deshalb künftig breiter gedacht werden: Bei der Prüfung von Geschäftspartnern geht es nicht mehr nur um Aspekte wie Lieferzuverlässigkeit und Qualität, sondern auch um IT-Sicherheit. Vor einer Zusammenarbeit gilt es, die Implikationen für die IT-Systeme der beiden

Geschäftspartner unter die Lupe zu nehmen. In der Folge sind die Systeme laufend auf Sicherheitsrisiken zu überprüfen.

Cyber Security Know-how aus der Schweiz für die Schweiz

Supplier Risk Management bedeutet künftig also vor allem auch Supplier Cyber Risk Management. Nur durch eine verstärkte Kooperation mit ihren Geschäftspartnern können Behörden und Unternehmen die gesamte Wertschöpfungskette sicher machen. Dafür braucht es Spezialisten, die Risiken professionell einschätzen und eindämmen. Idealerweise stammt das Know-how dafür aus der Schweiz. Denn für den Staat und die Wirtschaft gilt das gleiche wie für die Politik: Je mehr «Swissness» in der IT-Sicherheit drinsteckt, umso höher ist letzten Endes die Cyber-Souveränität.

CyOne Security ist der vertrauensvolle Partner dafür

Es gilt also, die Schweiz vor Cyber-Risiken zu schützen mit einer durchgängig schweizerischen Supply Chain. Denn eine moderne und effiziente Informations- und Kommunikationstechnologie bildet das Rückgrat von Staat und Wirtschaft und ist unabdingbar. Agil, skalierbar und mit einer gesicherten Verfügbarkeit trägt sie entscheidend zum nachhaltigen Erfolg und zur Wettbewerbsfähigkeit 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 und somit die Schweiz vor Cyber-Risiken zu schützen.

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

Kontaktieren Sie uns für ein kostenloses Expertengespräch.