VICCON

CONSULTING

Next Generation Security Management

Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements für die 4. Industrielle Revolution

Ein Leitfaden für CDO, CIO und CISO

IMPRINT

Broschüre: Next Generation Security Management - Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements für die 4. Industrielle Revolution

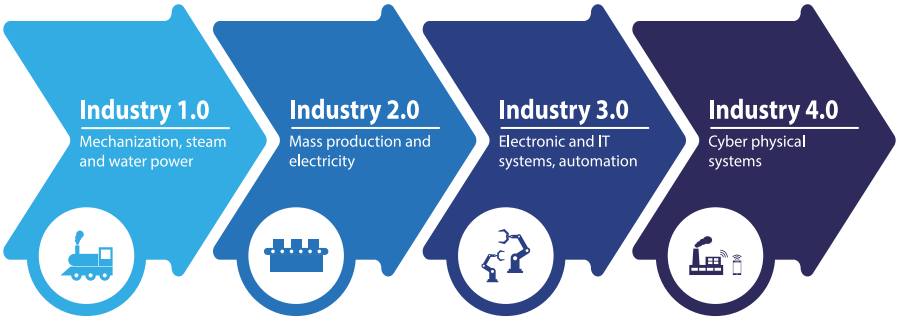
© 2019 VICCON GmbH

4. INDUSTRIELLE REVOLUTION UND DIGITALE TRANSFORMATION

Nachdem die Industrie in den letzten Dekaden weitgehend automatisiert wurde, haben die Vernetzungen und das Internet seit dem Jahr 2000 die Voraussetzungen geschaffen, eine weitere Evolutionsstufe in der Industrialisierung zu erreichen, die 4. Industrielle Revolution (kurz 4IR), die auch als Industrie 4.0 bezeichnet wird.

Wesentliches Merkmal dieser Stufe ist ein sehr hoher Automatisierungsgrad in der Produktion oder Nutzung sowie die Kommunikation der am Produkt beteiligten technischen Elemente, die selbständig untereinander über ihre Zustände und Aktivitäten informieren und gegebenenfalls autonome Entscheidungen treffen. Dies wird in der Zukunft vermehrt auf Basis von künstlicher Intelligenz passieren und mehr und mehr Services von Drittanbietern und auch die vernetzte Lieferkette einschließen. Neue Services veredeln oder individualisieren dabei das digitale Produkt. Elemente des vernetzten digitalen Produkts sind nicht nur die Anbindung ans Internet, die Bedienung mit einer App, sondern z.B. auch die Sammlung von Daten zu Zwecken der Nutzungsanalyse oder der vorhersagenden Wartung (Predictive Maintainance). Somit können diese digitalen Funktionen auch eine Sicherheitsrelevanz im Sinne von funktionaler Sicherheit bekommen. Cyber Security wird Teil von Functional Safety. Somit werden Cyber Security, Datenschutz und Informationssicherheit zentrale Elemente der 4. Industriellen Revolution. Dies erfordert eine durchdachte Digitalisierungsstrategie eines jeden Unternehmens, einerseits in der Wertschöpfungskette selbst, anderseits in einer gemeinsamen Steuerung dieser Themen, dem Security Management.

Die vorhersehbare und unvorhersehbare technische Entwicklung wird viele Branchen grundlegend transformieren. Um diese Veränderungen zu managen reichen zukünftig nicht mehr nur neue Rahmenwerke oder übergreifende Zusammenarbeit, sondern es bedarf auch angepasster Arbeitsmethoden und Prozesse sowie neuer Modelle zur Wissens- und Kompetenzvermittlung, die zu der Schnelllebigkeit des Marktes und der Arbeitskräfte passen.



CYBER NORMS UND HAFTUNG

Um die Situation, der man sich als Unternehmen ausgesetzt sieht, richtig verstehen zu können, muss einem bewusst sein, dass international aktuell für Staaten kein verbindliches Rahmenwerk zum Verhalten im Cyber-Raum existiert. Während die meisten Staaten den Cyber-Raum als militärische Domäne für sich erkannt haben, ist die UN bislang nicht in der Lage, ein einheitliches Verantwortungsbewusstsein der Staaten „Responsible State Behaviour" im Cyberspace zu vereinbaren und Cyber-Normen zu verabschieden. Cyber-Attacken sind somit in nicht allen Staaten verboten oder werden von deren Rechtssystem erfasst. Die eigene Haftung kann somit nicht auf den Täter abgewälzt werden. Eine Ahndung bei Schäden ist somit nicht immer möglich. Auch die Cyber-Abwehr ist in vielen Staaten nur für den behördlichen Sektor organisiert, nicht aber für den privaten. Entsprechende Cyber-Bedrohungsinformationen werden auf staatlicher Ebene nur sehr zurückhaltend mit der Wirtschaft geteilt. Das Schutzprinzip des Staates für die Abwehr militärischer oder staatlicher Angriffe auf die Wirtschaft ist im Cyberspace nicht wirksam gegeben. Threat Intelligence und Abwehrmaßnahmen und Täterverfolgung müssen Unternehmen daher selbst stemmen, obwohl die Attribution, also die Zuordnung der Herkunft von Cyber-Angriffen, von Unternehmen kaum zu lösen und zumeist politisch heikel ist. Entsprechender Kompetenzaufbau in diesen Feldern für die Wirtschaft wird auf Ebene der staatlichen Aus- und Weiterbildungsmöglichkeiten nur unzureichend abgebildet. Als Unternehmen muss man sich folglich auf einen professionellen Angreifer einstellen. Produkte und Dienstleistungen, die für Angreifer hinreichend attraktiv sind, müssen vom Unternehmen ausreichend geschützt werden, insbesondere, wenn sie eine Safety-Relevanz haben. Bei vernetzten Systemen und Services mit Dritten stellen die Risikoeinschätzung und das Einhalten eines einheitlichen Sicherheitsniveaus die Unternehmen vor große Herausforderungen.

Ein weiterer Aspekt ist neben den Datenschutzgesetzen der einzelnen Staaten oder Regionen der Umgang mit Daten, von denen Staaten verlangen, dass diese im Land verarbeitet und gespeichert werden. Das kann so weit gehen, dass bei wirtschaftlichen Schlüsseltechnologien das Land verlangt, nationale Verschlüsselungs- oder Kontrolltechnologie in die Unternehmensnetze einzubauen. Hinsichtlich des Datenschutzes gibt es den Ansatz, der zumeist im Westen vertreten wird, dass

personenbezogene Daten der entsprechenden Person gehören, während in anderen Teilen der Welt die Daten als Teil der Internetinfrastruktur gesehen und sie somit dem Einflussbereich des Staates zuordnet werden. In jedem Fall kann man erkennen, dass Daten und Cyberspace immer stärker politischem Einfluss unterliegen und immer mehr unter Kontrolle und Regulierung kommen. Verbote der Nutzung von verschlüsselter Kommunikation oder verwendeter Algorithmen durch Unternehmen ergänzen dies, ebenso wie Patente auf Software oder Einschränkungen in der Supply Chain. Dies kann die Nutzung bestimmter Cloud-Diensten andere Dienste von Drittanbietern betreffen. Deshalb sind bei Überlegungen zu digitalen Produkten solche Aspekte einzubeziehen und ganzheitlich zu durchdenken.

> *In jedem Fall kann man erkennen, dass Daten und Cyberspace immer stärker politischem Einfluss unterliegen.*

Cyber-basierte Sabotage, Spionage und Kriminalität wachen stetig und die Angreifer werden immer versierter. Je abhängiger das eigene Produkt von Cyberspace ist, desto wichtiger ist die Betrachtung aller dafür relevanten Aspekte in Form eines durchgängigen Ansatzes. Da Cyber-Angriffe bestehende Schwachstellen voraussetzen, die man bei Software-basierten Systemen einer bestimmten Komplexität grundsätzlich nicht vermeiden kann, beginnt die Betrachtung an dieser Stelle. Werden digitale Vorprodukte eingekauft und eingesetzt, ist dort eine bewusste Entscheidung zu den Risiken notwendig. Ist der Anbieter oder Hersteller vertrauenswürdig? Bietet die Komponente oder der Service ausreichend Sicherheit?

Diese Fragen sind nicht einfach zu beantworten, jedoch können damit verbundene Risiken über eine geeignete Risikomethodik im Unternehmen gesteuert werden. Auch bieten international anerkannte Zertifizierungen oder Referenzen digitales Vertrauen. Die Nachvollziehbarkeit solcher Unternehmensentscheidungen und der dazu gewählten Maßstäbe werden in Zukunft immer wichtiger, sei es für Produkthaftung, Versicherungen oder rechtliche Ermittlungen in Schadensfällen. Ein Sicherheitsmanagement kann dabei helfen, Organhaftung zu vermeiden. Diese kann eintreten, wenn Führungskräfte falsche Entscheidungen im unternehmerischen Handeln treffen, die einen Schaden bei Dritten verursachen. Ein Weg, digitale Produkte sicher in die Value Chain einzubeziehen, ist außerdem, einen ganzheitlichen Ansatz zu wählen, der die Business-IT, die IT in der Konzeptphase, in der Produktionsphase und in der Phase des Betriebs und der Wartung des Produkts umfasst.

Dies getrennt in Abteilungen und somit in Silos zu organisieren reicht heute aber nicht aus. Verfügbarkeit, Vertraulichkeit und Integrität laufen entlang von Arbeitsprozessen. Existieren Datenkommunikation und Datenverarbeitung über alle Bereiche hinweg, wie z.B. bei PLM-Systemen, müssen diese über alle Prozessschritte gesichert werden. Fließen CAD/CAM-Daten durch die Geschäftsprozesse und erzeugen Prototypen, so müssen die Führungskräfte diese gegebenen falls in den Geschäftsprozessen schützen. Wird Software für ein Produkt mit Business-IT entwickelt und durchläuft verschiedene Phasen des Herstellungs- und Wartungsprozesses, so sind die Sicherheits- und Qualitätsanforderungen an das Produkt schon bei Beginn in der Business-IT zu berücksichtigen. Bezogen auf Produkt-Lebensphasen kann es sein, dass ein Unternehmen überlegen muss, ein Produkt am Ende der Lebensdauer wieder vom Kunden zurückzunehmen, um das inhärente digitale Know-how zu schützen. Agile Arbeitsmethoden sind beliebt, bringen aber herkömmliche Know-how-Schutz-Methoden an ihre Grenzen. Dies ist nur mit einer ergänzenden Sicherheitskultur und unter Beachtung des Human Faktor zu leisten.

> *Verfügbarkeit, Vertraulichkeit und Integrität laufen entlang von Arbeitsprozessen.*

SICHERHEITSSTRATEGIE

Trends und Themen wie Resilienz, Vernetzte Gesellschaft und New Work müssen in zukünftige Überlegungen einfließen.

Während ein Sicherheitsmanagement üblicherweise den Anforderungen an die Organisation unterliegt und in die bestehenden Führungs-, Leistungs- und Unterstützungsprozessen integriert wird, bestehen an die Cyber Security bzw. IT-Sicherheit andere Anforderungen.

Der Ansatz, Cyber Security bzw. IT-Sicherheit auf die gleiche qualitative Ebene zu heben, wie die in der Produkterstellung, erscheint notwendig und erfolgversprechend. Das bedeutet, diese Disziplin auf der Ebene von ingenieurstechnischen Prinzipien, Methoden und Vorgehensweisen zu verorten und nicht mehr zu akzeptieren, dass die Sicherung von Software und IT vom zufälligen Wissensstand einzelner Mitarbeiter anhängt. Dazu ist eine geeignete Steuerung über das gesamte Unternehmen nötig. Diese kann zum Beispiel durch das Zusammenwirken des Chief Digital Officers (CDO), des Chief Information Officers (CIO) und des Chief Information Security Officers (CISO) geschehen.

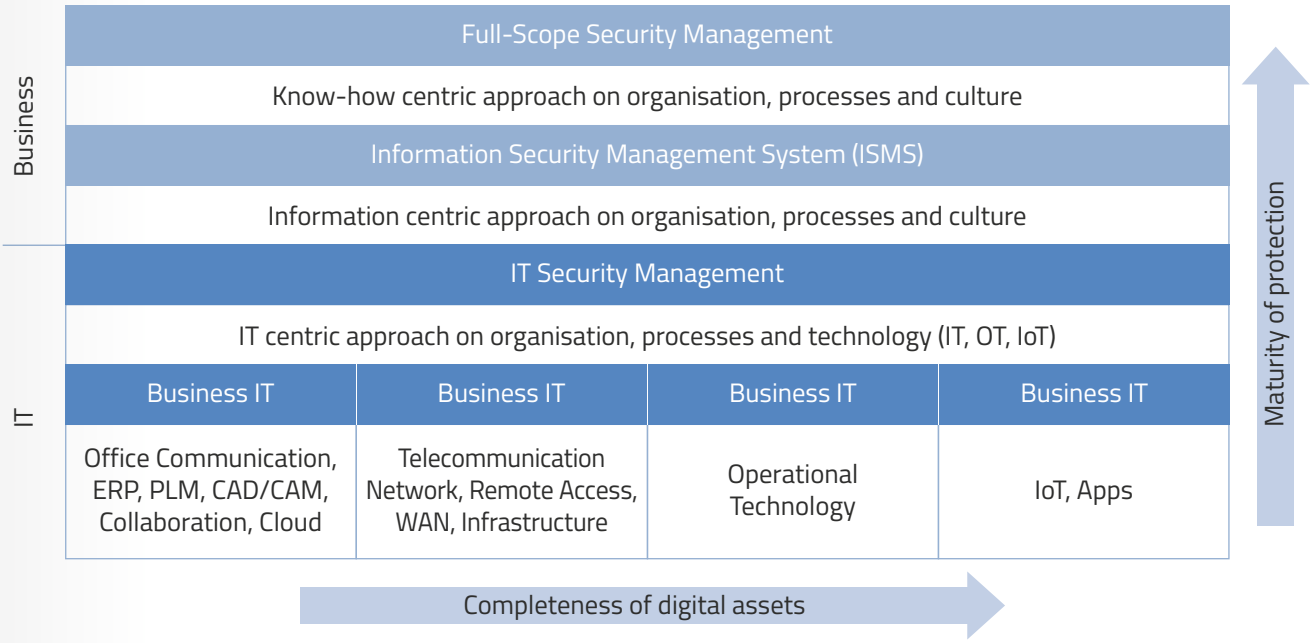
Während der Beitrag des CDO zur Sicherheit bei der digitalen Transformation insbesondere darin besteht, den sicherheitsverantwortlichen Stellen zu erklären, was die Sicherheitsanforderungen aus Sicht des Unternehmens und der Kunden sind, so hat der CISO die Aufgabe, unternehmensübergreifend Informationssicherheit so zu organisieren, so dass die Anforderungen des CDO über die Lebensdauer der Produkte und Services gewährleistet sind. Der CIO hat die Aufgabe, die Informationssicherheitsstandards des CISO in die IT-Projekte und IT-Services zu integrieren, die für digitale Produkte benötigt werden. Ideal ist, wenn es von allen drei Rollen entsprechende Strategien gibt, die in sich verzahnt sind, oder eine gemeinsame Strategie existiert.

Trends und Themen wie Resilienz, Vernetzte Gesellschaft und New Work müssen in zukünftige Überlegungen einfließen. VICCON verarbeitet solche Anforderungen in einer Sicherheitsstrategie, in der mit einem methodischen Ansatz konkrete Maßnahmen für die zukünftige Arbeit der Sicherheitsabteilungen und des gesamten Unternehmens abgeleitet werden.

NEXT GENERATION SECURITY MANAGEMENT

Die Kreativität von Angreifern im Cyberspace ist unerschöpflich. Unternehmen haben nur eine Chance, wenn Informationssicherheit geordnet funktioniert, also zum Beispiel über ein Sicherheitsmanagementsystem (SMS) organisiert ist, das Themen wie Know-how-Schutz, Informationsschutz und Cyber Security bzw. IT-Sicherheit adäquat abbildet und in die Risikobetrachtung des Unternehmens einschließt. Die Unternehmensführung wird über die Sicherheitsrisiken informiert und kann bewusste Entscheidungen dazu treffen.

Das VICCON Next Generation Security Management umfasst nicht nur einen ganzheitlichen Ansatz im Sinne eines Full-Scope Security Management, mit allen angesprochenen Aspekten, sondern ergänzt diese um ein bewährtes und stetig weiterentwickeltes Prozessmodell zum Security Management, das je nach Ausprägung bis zur Zertifizierung gebracht werden kann. Dieses Prozessmodell ist geeignet, die genannten Aspekte an die Bedürfnisse des Unternehmens anzupassen und in den internationalen Landesgesellschaften auszurollen und Sicherheit so zentral zu steuern. VICCON berät beim Aufbau oder Umbau eines Sicherheitsmanagements und liefert alle dafür notwendigen Services und Instrumente, national wie international.



ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

VICCON unterstützt seit rund 20 Jahren Organisationen darin, sicherheitsrelevante Entwicklungen zu verstehen, die notwendigen Kompetenzen und Prozesse dafür aufzubauen und sie so sicher zu beherrschen.

VICCON entwickelt mit Ihnen gemeinsam Ideen und sucht im Dialog mit allen Unternehmensebenen eine passende Orientierung zur Sicherheitspolitik im Lichte der unterschiedlichen Anforderungen.

VICCON entwickelt Strategien für sichere und resiliente Organisationen, begleitet die digitale Transformation und berät bei der Implementierung dieser Strategien in Form eines Next Generation Security Managements.

VICCON verfolgt das Ziel, Security im Sinne des Managements und Business im Unternehmen strategisch zu verankern. Besondere Schwerpunkte liegen im Informationssicherheitsmangement sowie im Management von Cyber-Risiken und im Prototypen- und Know-how-Schutz.

KONTAKT

Für weitere Informationen kontaktieren Sie:

VICCON GmbH

Ottostraße 1
76275 Ettlingen
Deutschland

Tel.: +49 7243 719734
Fax: +49 7243 719704

E-Mail: info@viccon.de
www.viccon.de

VICCON

CONSULTING