Gerhard Steininger
VP Sales & Business Development
bei der asvin GmbH, Stuttgart



## Cybersecurity ist wesentlicher Bestandteil des Due Diligence Verfahrens

**Cybersecurity ist zunehmend ein Grund für signifikante, operationale und finanzielle Risiken ganzer Unternehmen. Sie gehört dringend in den Bewertungsprozess für Übernahmen und Verkäufe. Denn Gefahrenpotenziale und Angriffsflächen für Cyber-Kriminelle entstehen nicht aus dem Nichts. Sie entwickeln sich durch riskante Vernachlässigung von Cyberrisiken, durch falsche Akzentuierung von Prioritäten und unter bewusster Vertuschung von Vorfällen oder aufgetretener Schäden im Vorfeld von Unternehmensverkäufen. Daher sollte das Thema Cybersecurity fest in Due Diligence Verfahren verankert sein.**

Am Beispiel des schwäbischen Batterieherstellers Varta wird deutlich, wie ein schwerwiegender Cyber-Vorfall entscheidenden Einfluss auf die Zukunft des Unternehmens und insbesondere auf den Verkauf von Unternehmenssparten nehmen kann. Varta war 2024 ein Sanierungsfall. Um die Zukunft des Unternehmens zu sichern, wurde ein Sanierungsfahrplan ausgearbeitet. Genau in dieser Phase erfolgte ein Ransomware-Angriff auf den bereits angeschlagenen Batteriehersteller. Die Produktion wurde wochenlang lahm gelegt, wodurch ein zweistelliger Millionenschaden verursacht wurde. Kosten und Schäden machten die bestehende Sanierungsplanung über Nacht obsolet. Zudem waren die Finanzplanungssysteme stillgelegt, was die Erstellung von belastbaren Kennzahlen und Bilanzierungen schlicht unmöglich machte. Nicht zuletzt führte dieser Cyber-Vorfall dazu, dass finanzierende Banken und Investoren ihr Vertrauen in das Unternehmen weiter verloren und die Krise bei Varta einen neuen Höhepunkt erreichte.

> *"How did you go bankrupt? Two ways: Gradually, then suddenly."*
> (Ernest Hemingway – The sun always rises)

Mirko Ross
Gründer und CEO
der asvin GmbH, Stuttgart



Ransomware-Angriffe sind die am häufigsten auftretenden Cybersecurity Angriffe. Nach vieler Expertenmeinungen ist es nicht die Frage, ob man Opfer eines Angriffs wird, sondern wann! Auch dieses Beispiel zeigt, dass das sich das Thema Cybersecurity oft noch nicht auf der Agenda der CEO befindet. Laut einer Ende August 2024 vom Digitalverband Bitkom veröffentlichten Umfrage, legte der wirtschaftliche Schaden durch Angriffe auf Betriebe im vergangenen Jahr um 29 Prozent auf 266,7 Milliarden Euro zu – ein neuer Höchstwert. Rund 267 Mrd. Euro Schadenssumme, ist ein enormer Betrag, der bei betroffenen Unternehmen an anderer Stelle für eine gesunde Geschäftsentwicklung fehlt.

**Die Cyber Security Due Dilligence (CSDD) fehlt auf der M&A-Agenda**

Insbesondere Unternehmen im M&A Fokus, die aufgrund von Sanierungsmaßnahmen oder schnellem Wachstum zum Verkauf stehen, haben grundsätzlich ein Problem damit, ausreichende Ressourcen für Cybersicherheit und die Umsetzung von notwendigen als auch präventiven Maßnahmen bereitzustellen. Daher sind Sicherheitslücken ein sehr ernstzunehmendes Risiko, das automatisch auf den Käufer übertragen wird. Das Einpreisen und Berücksichtigung solcher Cyberrisiken in die Verhandlungen findet im Prinzip nicht statt.

Wer hingegen Cybersicherheitsfragen bei M&A dagegen direkt in seinen Due Diligence (DD)-Verfahren einbaut, ist eindeutig auf der sicheren Seite. Beispiele hierfür sind indessen rar, weil entsprechende Praxis bisher schlicht nicht gelebt wird. Klar aber ist, dass sich durch rechtzeitiges Erkennen und Beseitigen von Angriffsvektoren Milliardenbeträge einsparen lassen.

Private Equity-Unternehmen, Banken und auch die Beratungshäuser haben den Trend erkannt und verstärken ihr Angebot durch dezidierte Cyberrisikoanalyse-Expertise. Das erklärte Ziel ist: Die Nachteile und Verluste durch Cyberrisiken methodisch zu quantifizieren, um diese als Parameter im Kaufprozess einpreisen und besser absichern zu können.

**Bedrohungen aus dem Cyber-Raum erfordern Cyber-Risikoanalyse in der Due Dilligence**

Schäden, Kontrollverluste und Imagebeeinträchtigungen durch Cyberangriffe werden in Summe sehr teuer für die angegriffenen Unternehmen. Hinzu kommt ein weiteres Problem: Angreifer bewegen sich im Schnitt 151 Tage *unbemerkt* im Unternehmen, bevor der Angriff erkannt wird. Genug Zeit, um Daten abzuziehen und die Ausführung von Ransomware vorzubereiten. Schlecht für Käufer von Unternehmen, wenn Risiken durch solche unerkannten Angriffen nach dem Verkaufsabschluss wirksam werden.

Hier herrscht daher dringender Handlungsbedarf insbesondere bei Aufkäufen und Zusammenschlüssen: Es muß eine grundsätzliche Neubewertung von Kosten auf die Due Diligence-Agenda. Sind Cybersecurity-Maßnahmen dort nicht thematisiert und eingepreist, steigen für Käufer im M&A-Prozess die Gefahren durch unvorhergesehene Kosten durch Cyberangriffe nach der erfolgten Übernahmen.

Eine für Cyberrisiken optimierte „Quick Strike" Analyse im Due Diligence Prozess kann hier frühzeitig Probleme erkennbar machen. – Sie weist auf kritische Bedrohungen hin, priorisiert und quantifiziert hier die unternehmenskritischen Segmente. Cyber-Resilienz lässt sich damit im Kaufprozess berücksichtigen.

**Den Wertschöpfungsfaktor durch Cyber-Security Due Diligence erkennen**

Cyber-Sicherheit wird bei M&A zum unverzichtbaren Faktor, und insgesamt als Wachstumsmodell erkannt. Dass Cyberresilienz seinen Wertschöpfungsbeitrag leisten, zum Alleinstellungsmerkmal reifen, oder gar zum Wettbewerbsfaktor werden kann, haben insbesondere Unternehmen in den USA erkannt und spielen hier eine Vorreiterrolle. Hier spielen die besonderen Haftungsrisiken, insbesondere bei Unternehmen unter Aufsicht der SEC, eine besondere Rolle. Unternehmen unter der Aufsicht der SEC sind verpflichtet die Auswirkungen von Cyberangriffen zu bewerten und die SEC formal in vorgegebenen Fristen zu informieren. Bei Nachlässigkeiten drohen empfindliche Sanktionen durch die Kapitalmarktaufsicht.

Außerhalb der USA werden Risiken durch Cyberangriffe oftmals noch zu stark ignoriert oder hingenommen. Der Anteil proaktiver Cyber-Risikovorsorge am IT(OT)-Etat liegt derzeit zwischen zehn und 15 Prozent. In sicherheitskritischen Branchen wie dem Finanzwesen oder der Gesundheitsbranche kann dieser Anteil allerdings höher liegen, oft bis zu 20 Prozent.

Nicht zu vernachlässigen im Cyber-Scherheitsmarkt ist zudem der Trugschluß fehlender Größe: Weil Cyber-Resilienz als schwierig darstellbar und nur zu hohen Extrakosten als realisierbar gilt, so die Annahme, könnten nur Großunternehmen oder solche, die als Betreiber kritischer Infrastruktur existenziell auf Resilienz angewiesen sind, hier investieren. Das stimmt zwar im alten Denkmuster, gilt aber unter den neuen Marktbedingungen nur noch bedingt. Heute ist Cyber-Sicherheit durch kluge Risikoanalyse und gut austarierte Ausgabenpriorisierung zu überschaubaren Kosten machbar. Gleichzeitig wird voreingestellte Cyber-Sicherheit zum wichtigen Alleinstellungsmerkmal.

**Cybersecurity „Quick Strike“ Due Diligence Framework**

Die folgende Abbildung zeigt einen Überblick des „asvin Cybersecurity Quick Strike Due Diligence Framework“. Prinzipiell ist das asvin-Framework in 4 Bereiche aufgeteilt.

- **Cybersecurity Management System:**
Die aktuelle Regularien erfordern häufig die Etablierung eines CSMS (Cybersecurity Management Systems), das ist oft ein Qualitätsmanagement System speziell für Cybersecurity. Dort werden Kern-Prozesse und deren Kontrollen beschrieben.

- **Cybersecurity Kern-Prozesse:**
Wichtig für die Abwehr und Erkennung von Angriffen ist ein regelmäßiges Testen der IT Komponenten. Hierfür werden Asset Management Daten mit Daten aus zuvor erstellten SBOM (SW Bills of Material) abgeglichen und eine Threat Intelligence aufgesetzt. Diese kontextbasierte Risikoanalyse inklusive Aufgaben-Priorisierung ist Kernfunktion der asvin-Lösung. Sie verschafft den perfekten Überblick auf die jeweilige Cyberbedrohungslage.

**▶ Cybersecurity Supply Chain:**
Viele Cyber-Vorfälle der letzen Jahre sind duch die Supply Chain verursacht worden. Mit am bekanntesten ist der sog. „Colonial Pipeline"-Angriff, bei dem durch einen Ransomware-Angriff das Billing-System ausgefallen ist, und dadurch die Ölversorung in großen Teilen der USA nicht mehr gewährleistet werden konnte.

**▶ IT/OT Security Architektur:**
Die IT ist schon lange den Gefahren durch Cyber-Angriffe ausgesetzt, die Operational Technology (OT) dagegen, also die Steuerung industrieller Anlagen, steht relativ neu im Fokus und ist verstärkt von Cybercrime betroffen. Eine gute Security Architektur zeichnet sich z.B. durch Vermeindung von Clusterbildung aus. Die Bewertung wird von dem *asvin IT Tool Risk by Context* durchgeführt.

**Cybersecurity „Quick Strike" Due Diligence Rahmenwerk** Abb. 1

| CYBERSECURITY MANAGEMENT SYSTEM (CSMS) | | | | |
|---|---|---|---|---|
| CSMS Governance | | | | |
| Kultur & Wahrnehmung | | | | |
| CS Risiko Management | Schwachstellen-Management | Produkt Monitoring | Zulieferer Security Management | Vorfalls Management |

| CYBERSECURITY SUPPLY CHAIN |
|---|
| Vertrieb – Einkauf |
| Lieferantenkette |
| Unternehmens Sicherheit |
| Behörden Berichte |

| CYBERSECURITY KERN PROZESSE |
|---|
| Testing |
| Asset Management – SBOM |
| Threat Intelligence |

| IT / OT RISK BY CONTEXT™ |
|---|
| Sicherheits Architektur |
| IT (Information Technology) |
| OT (Operational Technology) |

*Quelle: asvin.io*

**Cybersecurity Quick Strike Vorgehensweise**

Die nachfolgende Abbildung zeigt die schematische Vorgehensweise bei einer Cybersecurity Due Diligence. Die Vorgehensweise ist gegliedert in 5 Phasen und sollte nicht mehr als 2 Wochen benötigen.

**Cybersecurity „Quick Strike“ Ansatz** Abb. 2


** Traditional Security, Emerging Technology, Managed Security, CVSS Score, IT/OT, Threat Intelligence*

- **Phase 1 Scoping:**
  Anhand des Cybersecurity Frameworks wird der Scope mit den relevanten Stakeholdern definiert.
- **Phase 2 Identification:**
  Relevante Daten und ihre jeweiligen Quellen werden identifiziert.
- **Phase 3 Assessment:**
  Hier wird anhand relvanter Kriterien das Assessment durchgeführt.
- **Phase 4 Evaluation:**
  In dieser Phase werden die Daten mit den Kriterien in einen Kontext gebracht (Risk by Context) und idealerweise bereits verschiedenen Szenarien durchgespielt.
- **Phase 5 Priotization:**
  Im letzten Schritt werden die bestehenen Lücken und Vulnerabililitäten beschrieben. Gleichzeitig werden Handlungsempfehlungen daraus abgeleitet.

Ein sehr anschauliches Beispiel für die Notwendigkeit, Cyber-Sicherheitsanalysen in Unternehmensbewertungsverfahren einzubauen, ist der noch heute schwelende Rechtssteit um die Folgen des SolarWinds-Hacks mit dem sog. Sunburst-Trojaner. Bereits 2020 entdeckt, ist der Vorfall nach wie vor einer der weitreichendsten Cyberangriffe der jüngsten Zeit. Er offenbarte die Schwachstellen in der Sicherheitsinfrastruktur vieler großer Organisationen weltweit. Rund 18.000 Unternehmen waren betroffen. Noch Mitte Juli 2024 wies ein US-Bundesbezirksrichter zwar die meisten Ansprüche in einer Klage der US-Börsenaufsichtsbehörde SEC gegen SolarWinds ab. Aber der Vorgang legte signifikante Verstöße in Sachen Cybersicherheit offen. So wurde dem Unternehmen vorgeworfen, Investoren betrogen zu haben, weil es das Wissen über Cyber-Schwachstellen in seinen Systemen absichtlich vor besagter Sicherheitslücke, die 2020 entdeckt wurde, verheimlicht habe.

Die SEC verklagte das Unternehmen im Jahr 2023 mit der Begründung, dass es 2020 und zuvor bereits vorhandenes Wissen über Systemfehler in Unternehmenserklärungen und -unterlagen verschwiegen habe. Das habe den insgesamt fast zwei Jahre(!) laufenden Angriff (Hack) erst ermöglicht. Der US-Bezirksrichter Paul Engelmayer in Manhattan entschied jedoch, dass die Offenlegung nach der Entdeckung von Sunburst auf nachträglicher Einsicht beruhte und dass die SEC nur Betrugsvorwürfe für Handlungen verfolgen kann, die vor der Entdeckung von Sunburst begangen wurden.

**Resumé**

Das Thema Cybersecurity sollte dringend in die etablierten M&A-Prozesse aufgenommen werden.

Technologiebewertung ist bereits heute ein wesentlicher Bestandteil von Unternehmensbewertungen. Cybersecurity muss hier definitiv mit berücksichtigt werden. Nach Aussagen des MIT (Massachustes Institute of Technlogy) werden heute weltweit nur etwa 1% aller Cybersecurity Vorfälle berichtet. Das bedeutet, der verursachte Schaden, der heute nach offiziellen Statistiken bei 6 Trillionen liegt, ist um ein vielfaches höher.

Die Due Diligence bei M&A-Prozessen hat die Aufgabe ein Unternehmen zu bewerten. Cybersecurity sollte daher heute ein essenzieller Bestandteil dieser Bewertungen sein.

g.steininger@asvin.io | m.ross@asvin.io

***Über die Autoren:***

***Gerhard Steininger*** *ist VP Sales & Business Development bei der auf Cyberrisikomanagement spezialisierten asvin, Stuttgart. Vor seinem Einstieg bei asvin war Steininger u.a. Senior Manager bei Deloitte und hat dort u.a. Cybersecurity Projekte bei einigen Automobil OEMs geleitet. Davor war er Direktor bei Dassault Systems und global für MBSE (Model Based System Engineering) verantwortlich. Er hält einen Master in Physik von LMU (Ludwig-Maximilian-Universität) München.*

***Mirko Ross*** *ist Gründer und CEO der auf Cyberrisikomanagement spezialisierten asvin GmbH, Stuttgart. Auf Bundesebene nutzt er seine Einflussmöglichkeiten als Mitglied des Arbeitskreises Wirtschaftsschutz und Cybersicherheit im BDI (Bundesverband der Deutschen Industrie). Als Mitglied des BDI-Arbeitskreises Wirtschaftsschutz und Cybersecurity nimmt er Einfluß auf die Stellungnahmen des Verbands zu EU-Regulierungen wie Kritis-Verordnungen, NIS2-Direktive oder Cyber Resilience Act. Im Bundesministerium für Bildung und Forschung (BMBF) ist Ross bestellter Experte und Mitglied der „Strategischen Plattform digitale und industrielle Technologien in HORIZON Europe".*