# CYBERSICHERHEIT

## *in Supply Chains*

## *Executive Summary*

10
2023


Foto: ipopba · istockphoto.com

# *Cybersicherheit in Supply Chains – Fortschritte, Schwachstellen und beeindruckende Erfolgsbeispiele*

*Executive Summary*

Cybersicherheit bleibt eine der zentralen Herausforderungen für Unternehmen. Hackergruppen, die wertvolle Datenbestände stehlen, oder kritische IT-Systeme verschlüsseln, fügen der Wirtschaft großen Schaden zu. Dabei verbringen die Hacker teilweise über 100 Tage im Netzwerk des Unternehmens, um Schadsoftware zu installieren und für sie interessante Daten zu finden. Die Bundesvereinigung Logistik (BVL) hat in Zusammenarbeit mit der Universität der Bundeswehr München, der Otto-von-Guericke-Universität Magdeburg und den Unternehmenspartnern One Identity, Schunck Group und secida in einer umfangreichen Studie untersucht, wie sich Unternehmen heute entlang der Supply Chain aufstellen, um dieser Herausforderung zu begegnen. In diesem Rahmen wurde eine Befragung von über 150 Mitgliedsunternehmen der BVL durchgeführt.

Foto: anyaberkut · istockphoto.com


Foto: mesh cube · istockphoto.com

# ***Der Status Quo:*** *Trotz guter technologischer Basis sind Cyberkriminelle oft erfolgreich*

- Die befragten Unternehmen haben derzeit eine recht gute technologische Basis. In vielen Fällen wurde die IT-Infrastruktur kürzlich modernisiert. Eigene Rechenzentren und die Cloud werden gleichermaßen genutzt. Die IT wird in der Mehrheit der Unternehmen mit eigenen Personalressourcen betrieben.

- Cybersicherheit und IT allgemein sind wichtig: Die Absicherung gegen Cyberangriffe hat in den meisten Unternehmen hohe Priorität, und IT insgesamt wird durchweg als wesentliches Thema für die Geschäftsführung eingeschätzt.

- Cyberangriffe sind Alltagskriminalität geworden: fast die Hälfte der befragten Unternehmen gibt an, dass sie in den letzten 5 Jahren mindestens einmal Opfer von Cyberkriminellen geworden sind. Etwa ein Drittel war auch mehrfach betroffen.

- Unterschiedliche Bereiche der IT wurden von Cyberkriminellen angegriffen: Häufig waren Webseiten (30%) und sensible Daten (25%) das Ziel. Auch Datenverschlüsselung mit anschließender Erpressung (15%) kam häufig vor.

- Bei der Analyse der Angriffsfälle hat sich herausgestellt, dass es Angreifern oft gelungen ist, Beschäftigte im Unternehmen dazu zu bringen, Schadsoftware zu installieren (37%). Auch aus dem Internet zugängliche Schwachstellen waren ein gern genutztes Einfallstor (28%). Benutzerkennungen und Passwörter wurden in 15% der Fälle missbraucht.


Foto: Kenstocker · istockphoto.com

# *Aktuelle Maßnahmen:*

## *Auf Cyberangriffe wird meist kompetent reagiert*

- Nach einem Cyberangriff reagieren die befragten Unternehmen mit unterschiedlichen Maßnahmen, um die Cybersicherheit zu verstärken. Im Regelfall wird eine Kombination von technischen Maßnahmen (98%), verstärkten Mitarbeiterschulungen (83%) und neuen bzw. verschärften Richtlinien (66%) eingesetzt. In etwa der Hälfte der Fälle (48%) wird auch zusätzliches Fachpersonal eingestellt.

- Große Unternehmen setzen mit deutlich höherer Wahrscheinlichkeit auf eine Kombination dieser Maßnahmen. 75% der Unternehmen mit einem Umsatz von über 500 Mio. EUR setzen nach einem Cyberangriff auf zusätzliches Fachpersonal, die übrigen oben genannten Maßnahmen werden von ihnen jeweils zu mehr als 90% als Antwort auf einen Cyberangriff eingesetzt.

- Zur Cybersicherheit werden häufig auch Prozesse im IT-Betrieb angepasst. Auch hier sind größer Unternehmen führend. Während über 90% von ihnen sicherheitserhöhende Maßnahmen wie das Patching von Anwendungssoftware und Betriebssystemen oder das regelmäßige Erstellen von Backups einsetzen, ist dies im Mittelstand nur bei weniger als zwei Dritteln der Unternehmen der Fall. Ein ähnliches Bild ergibt sich bei Cybersicherheits-Schulungen.

- Cyberangriffe haben teilweise lange Betriebsstillstände zur Folge. Fast die Hälfte der Befragten (49%) gab an, dass die Wiederherstellung der Betriebsfähigkeit nach einem Cyberangriff mehrere Tage oder länger gedauert hat. 24% gab an, dass die Wiederherstellung der Betriebsfähigkeit sogar mehrere Wochen, Monate, oder über ein Jahr lang gedauert hat. Insbesondere bei kleinen Unternehmen mit wenig Kompetenz in der Cybersicherheit oder bei sehr großen Unternehmen mit komplexer IT-Landschaft dauert es lange, bis wieder gearbeitet werden kann.

# *These 1: Das Management nimmt seine Rolle in der Cybersicherheit unzureichend wahr*

- Das Management der befragten Unternehmen ist trotz der teilweise gravierenden Angriffsfolgen mit dem Schutz gegen Cyberangriffe mehrheitlich zufrieden.

- Obwohl eine Zugehörigkeit zur gesetzlich regulierten kritischen Infrastruktur deutlich höhere Anforderungen an das Management von Cyberrisiken stellt, kann ein Viertel der befragten Manager nicht sagen, ob das eigene Unternehmen zur kritischen Infrastruktur gehört, oder nicht. Dies ist ein Indikator für einen Mangel an relevantem Wissen zu Cybersicherheit auf der Managementebene.

- Über 40% der befragten Manager konnte nicht sagen, ob das Unternehmen gegen Cyberangriffe versichert ist, oder nicht. Hier wird ein gravierendes Wissensdefizit in Bezug auf das Management von Cyberrisiken deutlich.

- Auch bei anderen relevanten Themen wird deutlich, dass das Management in vielen Unternehmen zu wenig über die Cybersicherheit im eigenen Hause weiß. Zum Beispiel wissen 28% der Befragten nicht, ob das Unternehmen in den letzten 5 Jahren Opfer von Cyberangriffen wurde, und 18% wissen nicht, ob das Risikomanagement im Unternehmen IT-Risiken mitberücksichtigt.

- Die Frage, ob Cybersicherheit in der Verantwortung der IT liegt, oder ob alle Mitarbeitenden eine zumindest teilweise Verantwortung dafür tragen, wird in den meisten Unternehmen differenziert beantwortet. Aus Sicht der meisten Befragten teilen sich beide die Verantwortung.

- Zwei Drittel der befragten Unternehmen verfügen über Richtlinien und Regeln für die IT-Sicherheit, ein ähnlicher Prozentsatz hat die geschäftskritischen Informationen identifiziert. Aber nur jeweils ein gutes Drittel der Unternehmen steuert die Cybersicherheit über entsprechende KPIs oder führt Cybersicherheitsübungen durch. In Summe besteht hier noch viel Nachholbedarf.

Foto: Khanisorn Chaokla · istockphoto.com

- Technische Sicherheitslösungen wie Inventar-Datenbanken für die IT-Systeme, Multifaktor-Authentifizierung, Netzwerksegmentierung oder Logging der System- und Netzwerkzugriffe werden in größeren Unternehmen häufig eingesetzt, sind aber noch nicht der Standard. Die wichtige Überwachung der Datenkommunikation wird noch nicht in allen Fällen durchgeführt.

- Management-Teams, die ihre Rolle in Bezug auf Cybersicherheit noch nicht abschließend definiert haben, sollten dies – ggf. unter Einbeziehung zusätzlicher Expertise – nachholen. Die Verantwortung für das Management von Cyberrisiken kann nicht vollständig delegiert werden.

Foto: Peach_iStock · istockphoto.com

# ***These 2:*** *Je größer das Unternehmen, desto mehr Cybersicherheits-Fachwissen steht dem Management zur Verfügung*

- Größere Unternehmen nutzen generell die verfügbaren Schutzmaßnahmen der Cybersicherheit häufiger als kleine Unternehmen. Grund hierfür könnte sein, dass großen Unternehmen auch mehr Ressourcen zur Verfügung stehen.

- Sinnvolle, aber kostspielige Schutzmaßnahmen wie z.B. Penetration Test werden fast nur von größeren Unternehmen eingesetzt (bei Unternehmen mit Umsatz.
  >500 Mio. EUR zu 92%, bei Mittelständlern mit Umsatz <25 Mio. EUR/Jahr nur zu 11%)

- Insbesondere im Mittelstand (Umsatz <25 Mio./Jahr) sind Pläne für Cybersicherheits-Notfälle deutlich seltener verbreitet als bei größeren Unternehmen.

- Kleinere Unternehmen können zwar nur weniger Ressourcen und Budgets für Cybersicherheit aufwenden, sollten aber trotzdem die in der jeweiligen Situation zu priorisierenden Maßnahmen umsetzen.

# *These 3: Magische IT – Das Management vertraut auf die Lösungsfähigkeit der IT*

- Das Management schätzt die IT-Kompetenz im eigenen Haus mehrheitlich sehr hoch ein, daraus resultiert ein hohes Vertrauen in die Lösungsfähigkeit der IT. Dies führt zu einer starken Delegation des Themas Cybersicherheit an die IT.

- Cybersicherheits-Regeln und Policies werden in mehr als der Hälfte der Unternehmen nicht regelmäßig überprüft; eine entsprechende Managementverantwortung wird häufig nicht wahrgenommen.

- 80% der Unternehmen führen für Cyberrisiken ein Risikomanagement durch. Dieses ist aber im Regelfall an die IT oder externe Dienstleister delegiert. Eine stärkere Beteiligung des Managements wäre wünschenswert.

- Über 70% der Unternehmen verwenden IT-Lösungen, die den Zugriff auf Daten und Systeme regulieren, und sind auch überzeugt davon, dass sie sicherstellen können, dass Mitarbeitende nur Zugriff auf Daten erhalten, die sie für ihre Tätigkeit wirklich benötigen. Der Zugriff wird im Regelfall auch überwacht, so dass unbefugte Zugriffe unterbunden werden können. Die Verantwortung hierfür wurde im Regelfall an die IT delegiert.

- Zwei Drittel der Unternehmen haben einen weitergehenden Schutz für die Benutzerkonten von IT-Administratoren und Nutzern mit Zugriff auf kritische Daten (Management, HR, F&E) etabliert, da diese Konten von besonderem Interesse für Hacker sind. Für dieses technische Thema liegt die Verantwortung sinnvollerweise bei der IT.

- Cybersicherheits-Awareness-Trainings sind in fast drei Viertel der Unternehmen heute Standard. Die übrigen Unternehmen sollten eine Einführung dieser vergleichsweise kostengünstigen Schutzmaßnahme prüfen. Der Einkauf entsprechender externer Online-Trainings kann auch von der IT gesteuert werden.

- Dedizierte Budgets für Cybersicherheit sind bisher nur in knapp zwei Drittel der Unternehmen etabliert. Die Verwaltung dieser Budgets ist an die IT delegiert, die Festlegung der Budgethöhe muss aber Managementaufgabe bleiben.


Foto: ra2studio · istockphoto.com

- Mehr als ein Drittel der Unternehmen hat bislang keine Planung für die Fortsetzung des Geschäftsbetriebs bei Ausfall von IT-Systemen durch einen Cyberangriff getroffen. Die Verantwortung für diese Planungen (Business Continuity Management) liegt im Regelfall bei der IT. Den Unternehmen, die sich mit dieser Thematik noch nicht auseinandergesetzt haben, wird geraten, dies in angemessenem Umfang nachzuholen. Die Unternehmen, die die Zuständigkeit für das Business Continuity Management an die IT vergeben haben, sollten sich fragen, ob es sich hier nicht primär um eine Verantwortung handelt, die Fachfunktionen auf der Geschäftsseite wahrnehmen sollten.

- Generell zeigen die Studienergebnisse, dass Cybersicherheit derzeit in einem zu hohen Grad an die IT delegiert wird. Geschäfts- und Funktionsleitungen sollten Themen, die nicht sinnvoll von der IT verantwortet werden können – beispielsweise Business Continuity Management – wieder in die eigene Verantwortung übernehmen, und die IT dort jeweils nur als Unterstützungsfunktion nutzen.


Foto: metamorworks - istockphoto.com

# ***These 4:*** *Supply Chains in Deutschland sind noch nicht genug abgesichert*

- Unternehmen betrachten Cybersicherheit mehrheitlich noch nicht für die gesamte Lieferkette. Nur 42% der Unternehmen geben an, dies schon heute zu tun. Insbesondere kleine und besonders große Unternehmen haben hier noch keinen Überblick.

- Die befragten Unternehmen betrachten den Schutz ihrer eigenen Materialflüsse gegen Cyberangriffe mehrheitlich als zufriedenstellend. Kleine und besonders große Unternehmen sind diesbezüglich deutlich skeptischer.

- Die Absicherung der Materialflüsse der eigenen Kunden ist bislang kein Schwerpunkt für die Cybersicherheit im Unternehmen. Ausnahme sind Unternehmen mit einer Umsatzgröße von 25-100 Mio. EUR aus der Zuliefererindustrie, die die Materialflüsse des Kunden deutlich stärker in den Fokus nehmen.

- Die Absicherung von Materialflüssen der eigenen Lieferanten spielt für die befragten Unternehmen derzeit noch eine sehr geringe Rolle. Im Vergleich mit der Absicherung der eigenen Materialflüsse oder der der Kunden ist die Absicherung in Lieferantenrichtung nochmal deutlich weniger etabliert.

- Lieferkettenübergreifende Pläne für Cybersicherheits-Notfälle sind noch kein Standardinstrument. Solche Ansätze sind erst im Aufbau.

- Generell ist die unternehmensübergreifende Absicherung gesamter Lieferketten gegen Cyberangriffe bislang ein Randthema für die befragten Unternehmen. Hierauf sollte deutlich mehr Fokus gelegt werden, da Hacker vermehrt ganze Supply Chains analysieren, und gezielt gegen die Unternehmen mit der schwächsten Absicherung vorgehen.

# ***These 5:*** *Supply Chain Cybersecurity Leaders verbinden überdurchschnittlichen wirtschaftlichen Erfolg mit einer deutlich höheren Performance in der Cybersicherheit*

- Unter den befragten Unternehmen konnte eine Gruppe identifiziert werden, die sich durch besonderen wirtschaftlichen Erfolg auszeichnet.
- Es fällt auf, dass diese Gruppe von Unternehmen deutlich öfter wichtige Cybersicherheits-Maßnahmen im Unternehmen umsetzt, als die übrigen Unternehmen. Der Abdeckungsgrad vieler Maßnahmen liegt in dieser Gruppe bei über 90%.
- Unternehmen in der wirtschaftlich erfolgreichen Gruppe verfügen auch deutlich häufiger als andere über ausgearbeitete Cybersicherheits-Strategien und -Notfallpläne.
- Es fällt auf, dass diese Unternehmen sich auch in viel stärkerem Maß um die Sicherheit ihrer Supply Chains kümmern, als andere Unternehmen. Die Unternehmen in dieser Gruppe beziehen insbesondere auch ihre Lieferanten in ihr Cybersicherheits-Konzept ein, und entwickeln deutlich häufiger als andere auch Cybersicherheits-Notfallpläne für die gesamte Lieferkette. Diese Unternehmen werden daher als Supply Chain Cybersecurity Leaders bezeichnet.
- Die hohe Cybersicherheits-Performance der Supply Chain Cybersecurity Leader zahlt sich aus: Diese Unternehmensgruppe wird deutlich seltener gehackt als der Durchschnitt aller Unternehmen. Die Wiederherstellung der Betriebsfähigkeit nach einem erfolgreichen Cyberangriff dauert bei ihnen deutlich weniger lange, als bei anderen Unternehmen.

Foto: Sitthiphong · istockphoto.com

- Eine gute Cybersicherheits-Performance wirkt sich also nicht nur nicht negativ auf den wirtschaftlichen Erfolg aus, sondern erhöht messbar den Schutz gegen Cyberangriffe. Andere Unternehmen sind aufgefordert, dem Beispiel der Supply Chain Cybersecurity Leader zu folgen.

**Berlin,**
**im Oktober 2023**


FI
CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München


ONE IDENTITY
by Quest


LEHRSTUHL
PSA
PRODUKTIONSSYSTEME
und –AUTOMATISIERUNG


SCHUNCK
GROUP


secida