# 1 Zusammenfassung

Die Forschung von Greenbone Networks zu den Schlüsselfähigkeiten, die hochgradig widerstandsfähige Unternehmen auszeichnen, hatte und hat folgende Ziele:

- *Erfahrungen von Unternehmen mit Cyberangriffen zu analysieren*
  Die Erfahrungen mit Cyberangriffen müssen ausgewertet werden, um eine gültige Grundlage für die Aufdeckung der Unterscheidungsmerkmale zwischen hoch und weniger widerstandsfähigen Unternehmen zu schaffen.
- *Verständnis über die verschiedenen Fähigkeiten erlangen, auf die sich Unternehmen verlassen, um Cyberangriffe zu verhindern, zu bewältigen, abzuschwächen und sich von ihnen zu erholen*
  Zu verstehen, welche Fähigkeiten am häufigsten vorhanden sind, seien sie technischer oder organisatorischer Natur.
- *Identifizierung von Fähigkeiten und anderen Merkmalen, die widerstandsfähigere Cyber-Unternehmen von anderen unterscheiden*
  Erkennen, welche der gebräuchlichsten Fähigkeiten einen Einfluss haben
- *Testen verschiedener Hypothesen über die wichtigsten organisatorischen Fähigkeiten, die die Cyber-Resilienz vorantreiben*
  Überprüfung unserer anfänglichen Annahmen darüber, welche Fähigkeiten das sein werden, insbesondere jene, die sich auf die Verwaltung von Geschäftsprozessen und Vermögenswerten beziehen.
- *Den Grad zu erkennen, in dem Cyber-Resilienz entweder als Geschäftsrisikoproblem oder als Technologierisikoproblem oder als beides betrachtet wird*
  Abschließend sollten die wirklichen Interessenvertreter identifiziert und die Frage beantwortet werden, ob Cyber-Resilienz mit technischen und/oder organisatorischen Maßnahmen gelöst wird. Zusätzlich wurde die Kostendifferenzierung betrachtet.

Unsere Forschung wurde von Frost & Sullivan im Frühjahr/Sommer 2019 durchgeführt. Befragt wurden 370 Organisationen für kritische nationale Infrastrukturen (CNI) in fünf der größten Volkswirtschaften der Welt, die 41,2 % des weltweiten BIP ausmachen (USA, Großbritannien, Frankreich, Japan und Deutschland). 52 % der Befragten waren in der Geschäftsleitung oder im C-Level-Management tätig. Die durchschnittliche Anzahl der Mitarbeiter betrug 13.500, und der durchschnittliche Umsatz lag bei 1,84 Mrd. USD, verglichen mit einem durchschnittlichen IT-Budget von 110 Mio. USD. In der Untersuchung wurden die Sektoren Energie, Finanzen, Gesundheitswesen, Telekommunikation, Transport und Wasserversorgung abgedeckt. Ausführliche demografische und firmografische Angaben sind in den Anhängen zu finden.

### Anmerkung des Herausgebers

Ursprünglich hatten wir geplant, diese Forschung im Herbst 2019 zu veröffentlichen. Während wir die Forschungsergebnisse anhand von Beispielen aus der Praxis erweiterten, nahm unsere Arbeit eine wichtige Wendung, als wir über 30 Millionen ungeschützte medizinische Unterlagen in Archiven auf der ganzen Welt entdeckten. In der Zwischenzeit haben wir einige spezifische Forschungsergebnisse über die Rolle und Verwundbarkeit medizinischer Bildarchive, so genannter PACS-Server (Picture Archiving and Communication System), veröffentlicht. Diese Arbeiten finden Sie hier[1]. Die Lage bleibt weiterhin besorgniserregend, da es heute noch mehr als 500 ungeschützte PACS-Server auf der Welt gibt.

### Über Greenbone Networks

Greenbone Networks wurde 2008 gegründet und ist ein führender, globaler Anbieter von Lösungen für Resilienz- und Schwachstellenmanagement. Der Greenbone Security Manager in seinen verschiedenen Formen – einschließlich dem Greenbone Vulnerability Manager (früher OpenVAS) – wird in mehr als 30.000 Installationen und Integrationen in einer Vielzahl von Branchen und Unternehmensgrößen eingesetzt. Er wurde mehr als 2,5 Millionen Mal heruntergeladen. Greenbone Networks hat seinen Hauptsitz in Osnabrück, Deutschland.

[1] Greenbone Security Reports, published September 2019 and December 2019 and corresponding status updates https://www.greenbone.net/en/blog/

# 2 Zusammenfassung der Ergebnisse

**Sind wir widerstandsfähig gegen Cyber-Attacken?**

Die Frage, ob eine Organisation eine hohe Cyber-Resilienz aufweist oder nicht wird mit zunehmender Häufigkeit und Intensität diskutiert. Der Begriff selbst wird in den Medien, in Regierungsstrategien und Herstellerdokumenten mehr und mehr verwendet. Trotz dieser wachsenden Aufmerksamkeit gibt es einen Mangel an Klarheit und Verständnis darüber, was Cyber-Resilienz ist – schützt sie unsere Unternehmen auf eine intelligentere Art und Weise? Wie erreichen wir sie? Wie erhalten wir sie aufrecht? Machen wir es besser als unsere Mitbewerber?

Unsere Studie, ihr Ansatz und ihre Ergebnisse geben eine Antwort auf all diese Fragen. Basierend auf einer wissenschaftlichen Definition von Cyber-Resilienz, ihren Elementen und Zielen, unterscheidet die Studie das Konzept der Cyber-Resilienz von anderen Informationssicherheitssystemen. Und – was am wichtigsten ist – sie befasst sich mit ihrer Umsetzung.

Als ein Konzept konzentriert sich die Cyber-Resilienz auf das wahre Ziel einer Organisation: ihr geplanter Erfolg. Diesem "beabsichtigten Ergebnis" nähert man sich, indem man digitale Sicherheit in die Geschäftsprozesse einbaut, die den von einer Organisation erbrachten Mehrwert erzeugen. Dabei werden die für sie kritischen Vermögenswerte als Priorität betrachtet, ohne an den Grenzen eines Unternehmens aufzuhören, das Teil einer Lieferkette ist. Sie schützt die Erbringung eines Mehrwertes durch die Organisation, nicht nur ihre IT-Systeme.

Auf der Grundlage dieses Verständnisses haben wir Organisationen aus sechs Sektoren im Bereich der kritischen nationalen Infrastruktur (CNI), die in fünf Ländern auf drei verschiedenen Kontinenten angesiedelt sind und über 40 % des weltweiten BIP abdecken, befragt und bewertet. Die Teilnehmer waren meist in Führungspositionen tätig.

**Regional unausgeglichene Cyber-Resilienz**

Unsere Ergebnisse zeigen, dass insgesamt nur 36 % der Organisationen in hohem Maße cyber-resistent sind. Die USA schneiden mit 50 % besser ab, wobei die europäischen Länder nahe am Durchschnitt liegen und Japan mit 22 % der CNI-Organisationen, die sehr widerstandsfähig sind, im Rückstand liegt.

**Unausgewogene Cyber-Resilienz in den verschiedenen Industriesektoren**

Die sechs CNI-Sektoren, die in diesem Bericht untersucht wurden – Energie, Finanzen, Gesundheit, Telekommunikation, Transport und Wasserversorgung – zeigen auch große Unterschiede in ihrer Erfahrung im Umgang mit Cyber-Angriffen, in der Art und Weise, wie sie bewährte Praktiken umsetzen, und in ihrem allgemeinen Status der Cyber-Resilienz. 46 % der Organisationen im Finanz- und Telekommunikationssektor sind in hohem Maße cyber-resistent, während nur 32 % im Energiesektor und 22 % im Transportsektor auf diesem Niveau liegen. Über alle Regionen hinweg befinden sich die Bereiche Gesundheit (34 %) und Wasser (36 %) nahe am Durchschnitt.

Darüber hinaus wurden die Teilnehmer von uns auch zu ihren bestehenden Geschäftsprozessen befragt. So konnten wir diejenigen Geschäftspraktiken identifizieren, die wirklich dazu beitragen, die Cyber-Resilienz eines Unternehmens zu verbessern. Neben der notwendigen Fähigkeit, kritische Geschäftsprozesse zu erkennen, zeigen die Antworten, dass die Fähigkeit, das entsprechende Persona (sowohl IT- als auch Nicht-IT-Mitarbeiter) zu mobilisieren, wenn ein geschäftskritischer Vermögenswert oder Prozess in Gefahr ist, einer der größten Unterschiede zwischen Unternehmen mit hoher und niedriger Cyber-Resilienz ist.

**Hohe Cyber-Resilienz ist keine Frage des Budgets**

Während die von uns untersuchten cyber-resistenten Unternehmen einen größeren Umsatz und ein größeres IT-Budget haben, zeigen die Ergebnisse im Detail, dass Cyber-Resilienz keine Frage des Budgets ist. Ausschlaggebend sind stattdessen gute Geschäftspraktiken in allen Bereichen sowie ein gründliches Verständnis der geschäftskritischen, digitalen Ressourcen und der Geschäftsprozesse sowohl für das Personal der IT-Sicherheit als auch für das Betriebspersonal. Wenn dies beherrscht wird, wird die

Aufrechterhaltung eines hohen Maßes an Cyber-Resilienz von 43% der Unternehmen, die bereits über eine hohe Widerstandsfähigkeit verfügen, in erster Linie als ein Technologieproblem angesehen.

**11 Fähigkeiten verbessern die Cyber-Resilienz um den Faktor sechs**

Unsere Untersuchung identifizierte drei Gruppen von Fähigkeiten die, wenn sie von einem Unternehmen genutzt werden, die Cyber-Resilienz dessen um den Faktor zwei, drei und sechs erhöhen. Wenn sie als Aktionsplan verwendet werden, kann ein Unternehmen seinen Reifegrad erhöhen und gleichzeitig in der Lage sein, ein hohes Maß an Cyber-Resilienz aufrechtzuerhalten.


Es ist diese Darstellung, die den größten Nutzen für Leser dieses Berichts bringt. Wir gehen davon aus, dass sie dazu beiträgt, ein hohes Maß an Cyber-Resilienz in der Organisation zu erreichen und aufrechtzuerhalten.

Dr. Jan-Oliver Wagner

CEO von Greenbone Networks