



carmasec
security. done. right.

“Wirtschaftsspionage und Erpressungstrojaner
auf dem Vormarsch - wirksame Methoden für
einen wehrhaften Mittelstand”

Interview von Entscheider kompakt mit
Carsten Marmulla, Senior Trusted Advisor carmasec

Entscheider kompakt ist das Online-Magazin des DIGITAL FUTUREcongress, der am 05.11.2019 in Essen stattfindet. Im Interview spricht Entscheider kompakt mit Carsten Marmulla, Senior Trusted Advisor der carmasec Ltd. & Co. KG über Wirtschaftsspionage, Kompromittierung von Daten und Infrastrukturen sowie Beeinträchtigung von IT-Systemen durch Erpressungstrojaner.

carmasec wird als Aussteller auf dem DIGITAL FUTUREcongress teilnehmen. Zudem können Interessierte am Workshop „Digitalisierungsrisiken minimieren“ teilnehmen.

Entscheider kompakt: Es vergeht praktisch kaum ein Tag, bei dem nicht mittelständische Unternehmen Ziel von Wirtschaftsspionage oder Cyber-Kriminalität werden. Warum sind die Daten gerade auch mittelständischer Unternehmen für die Angreifer so interessant?

Carsten Marmulla: Grundsätzlich sind nicht alle Cyberangriffe gezielte Angriffe – bei den aktuellen Erpressungstrojanern (Ransomware) kann man das gut sehen, diese Form der Attacken geht in die Breite vergleichbar zu Spam, weil es genügend Opfer gibt, die auch bereit sind zu zahlen, weil eben keine funktionierenden und getesteten Datensicherungen vorhanden sind. Dazu kommt bei gezielten Angriffen noch, dass Unternehmen häufig in mehr oder weniger komplexe Lieferketten eingebunden sind und nicht selten als Zulieferer für große Konzerne aus der Perspektive einer IT-Sicherheitsanalyse das schwächste Glied in der Kette sind und dementsprechend attraktiv für Cyberangriffe sind, da der Erfolgsfaktor für den Angreifer recht hoch ist.



Carsten Marmulla, Senior Trusted Advisor carmasec Ltd. & Co. KG

Entscheider kompakt: Viele Unternehmen haben sich in den letzten Jahren auf den Weg der Digitalisierung gemacht. Was ist der Grund, dass das Thema Cybersicherheit und die damit verbundenen Digitalisierungsrisiken oft unterschätzt werden?

Carsten Marmulla: Die Digitale Transformation betrifft als Querschnittsthema grundsätzlich alle Branchen, auch die Unternehmen, die bislang eher wenig IT-Kompetenz benötigten. Außer Frage steht, dass die Digitalisierung gewaltige Vorteile für Kosteneinsparungen, Prozessoptimierungen oder auch für die Gestaltung von komplett neuen Geschäftsmodellen bietet – sie erfordert aber einen fachlich-kompetenten Umgang mit damit verbundenen Risiken. Das Lukas-Krankenhaus ist ein Beispiel dafür, was schief gehen kann, wenn man die Vorteile der Digitalisierung umsetzen möchte ohne die Schattenseiten im Vorfeld analysiert und berücksichtigt zu haben.

Entscheider kompakt: Was würden Sie Unternehmen raten, um sich insbesondere vor Wirtschaftsspionage zu schützen?

Carsten Marmulla: Es gibt in der Informations- und IT-Sicherheit keinen 100%igen Schutz, es geht um einen risikobasierten Ansatz – es ist schlichtweg unwirtschaftlich alle Risiken mit technischen und organisatorischen Maßnahmen zu mindern. Es geht an vielen Stellen darum, ein unternehmens- und unternehmerspezifisches Risikoprofil zu identifizieren und anschließend pragmatische Maßnahmen zu definieren und umzusetzen. Es verbleibt daher immer ein individuelles Restrisiken, welches die Unternehmensleitung kennen und akzeptieren muss. Internationale Wirtschaftsspionage ist kein Hobby von Skript-Kiddies, sondern wird hochprofessionell von ausländischen Nachrichtendiensten als Auftragsleistung erbracht, allein bei dem Jahresbudget der NSA ist klar, dass dies ein sehr ungleicher Kampf ist – umso wichtiger wird die Identifikation und Dokumentation von Unternehmensrisiken und Vermögenswerten, die hiervon betroffen sein könnten. Kompletzt zu verhindern sind solche Angriffe allerdings nicht, eine gute Vorbereitung auf den Ernstfall kann allerdings im Krisenfall die Existenz des Unternehmens retten.

Entscheider kompakt: Trojaner werden oft über Mitarbeiter oder Anhänge im Unternehmen eingeschleust. Dort verbleiben sie zum Teil mehrere Monate bevor Sie dann anfangen ihr Unheil zu treiben. Was können Sie Unternehmen empfehlen, um sich gerade auch in der Verbindung Datensicherung und Trojanern besser zu schützen?

Carsten Marmulla: Es gibt verschiedene Handlungsstrategien, um diesen Bedrohungen zu begegnen. Gartner hat vor einigen Jahren beispielsweise CARTA als Methodik vorgestellt, um Vertrauen und Kontrolle in IT-Umgebungen zu steuern – Forrester hat kurze Zeit später das Zero-Trust-Modell definiert, welches grundsätzlich allen Endgeräten misstraut. Pragmatisch können aber auch klassische Ansätze wie Netzsegmentierung, Funktionstrennung und als absolute Basis eine funktionsfähige und regelmäßig getestete Datensicherung helfen, die Auswirkungen und Schäden solcher Angriffe zu verhindern oder zu mindern.



Carsten Marmulla zu "DevSecOps & Security Automation" auf dem ISD 2019

Entscheider kompakt: Die Unternehmen erleben hohe regulatorische Anforderungen hinsichtlich Compliance und Datenschutz. Von außen betrachtet ist es dennoch wie ein Wettrennen zwischen Hase und Igel! Welche 3 wesentlichen Empfehlungen für eine erhöhte Sicherheit für mittelständische Unternehmen können Sie geben, um eine erhöhte Sicherheit zu erreichen?

Carsten Marmulla: Die Einhaltung von regulatorischen Anforderungen ist eine Pflichtaufgabe und keine Kür! Es gibt hier keinen Verhandlungs- sondern nur einen Gestaltungsspielraum. Konkret gibt es eine ganze Reihe von Methoden und Vorgehensweisen, die auch für kleine Budgets Lösungsansätze liefern – sie es aus den BSI-Dokumentationen, der ISO 27001, speziell für KMU gestaltete Methodenbaukästen wie der ISIS12 oder branchenspezifische Anforderungen wie TISAX, PCI-DSS oder andere. Meine persönliche Empfehlung wäre in erster Linie immer eine spezifische Risikoanalyse als Basis für die Definition und Umsetzung von technischen und organisatorischen Maßnahmen – das kann im Zweifelsfall auch „nur“ die Härtung von kritischen Systemen sein beispielsweise in Form einer sicheren Konfiguration, die Funktionstrennung bei Benutzerkonten oder die Segmentierung von Netzen.

Entscheider kompakt: Stichwort IT-Compliance, darunter versteht man die gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft. Was hat den mittelständischen Unternehmen die Datenschutz-Grundverordnung gebracht und welche Maßnahmen empfehlen Sie heute dringend, um hier auf der sicheren Seite zu sein?

Carsten Marmulla: Wir haben im Frühjahr gezielt zu diesem Themenkomplex eine Studie durchgeführt, inwieweit Digitalisierung und DS-GVO zusammenpassen oder vielleicht sogar Gegensätze sind. Interessant war, dass die Mehrheit der Befragten bekundet hat, dass die DSGVO eher als förderlich für die Digitalisierung eingeschätzt worden ist. Vielleicht deshalb, weil die EU-DSGVO ein Exportschlager ist und wir es geschafft haben, europaweit ein einheitlich hohes Schutzniveau für personenbezogene Daten zu schaffen und damit einen konträren Ansatz zu den USA und China zu liefern. Meine Interpretation lautet: erfolgreiche Digitalisierung und rechtskonformer Datenschutz müssen keine Gegensätze sein, wenn man weiß, wie es geht und frühzeitig die entsprechenden Anforderungen im Entwicklungsprozess definiert.

Entscheider kompakt: Auf dem Digital FUTUREcongress am 5. November sind Sie mit von der Partie. Was werden Ihre Besucher auf dem Messestand erleben können?

Carsten Marmulla: Wir sind mit unseren Fachexperten vor Ort und bieten sowohl an unserem Stand (Halle 8, Nr. A 21) als auch in einem gesonderten Workshop-Format Orientierung und Unterstützung, um Digitalisierungsprojekte erfolgreich und sicher durchführen und abschließen zu können. Wir können unseren Besuchern daher direkt vor Ort erste Lösungs- und Beratungsansätze liefern und Empfehlungen mitgeben.

Entscheider kompakt: Herzlichen Dank für dieses wirklich spannende Gespräch!