Interview mit Marco Marchesi,
Verwaltungsratspräsident CymbiQ Group

Cyber Security hat höchste Priorität

Im Gespräch mit Marco Marchesi wird deutlich, welchen Risiken Firmen bei der zunehmenden Digitalisierung ausgesetzt sind. Welche Massnahmen zur Bekämpfung dazu ergriffen werden müssen, erläutert der IT- und Cyber-Security-Experte.

Interview: Monika Schläppi, Fotos: Nicolas Zonvi

Sie beschäftigen sich seit 25 Jahren mit IT- und Cyber Security. Ist das heute eine boomende Branche?

Marco Marchesi: Es ist fast schon zu einer Hype-Branche geworden. Seit den vergangenen sieben, acht Jahren wird das Thema vermehrt wahrgenommen. Wir haben bereits vor Jahren immer wieder auf die bestehenden Risiken hingewiesen. Tatsache ist, dass mit der fortschreitenden Digitalisierung, die Abhängigkeit von Daten und elektronischen Prozessen zunimmt. Das heisst, wir als Gesellschaft realisieren nach und nach, wie abhängig, oder noch schlimmer, wie verletzlich wir damit geworden sind.

Wenn Gaspipelines in den USA angegriffen werden, überrascht mich das nicht. Es war eine normale Ransomware-Attacke auf eine kritische Infrastruktur, etwas, das wir hier in der Schweiz in zunehmendem Masse ebenfalls erleben. Bereits 2014 hat ein Hackerangriff das ukrainische Stromnetz für zwei Tage lahmgelegt. Angriffe auf kritische Infrastrukturen sind bereits länger bekannt und gefürchtet.

Lange Zeit haben IT-Anbieter oder Smart-Home-Anbieter nicht eingesehen, dass die Sicherheit ein wesentlicher Aspekt ist und auch mitberücksichtigt werden muss. Man kann sagen, dass sie es zum Teil bis heute noch nicht ganz realisiert haben. Oder anders formuliert: Funktionalität vor Sicherheit.

Gemäss der UNO-Organisation ITU (Internationale Fernmeldeunion) sollen sich die Schäden durch kriminelle Handlungen im Jahr 2021 auf sechs Billionen Dollar belaufen?

Der Cyber-Crime-Markt ist mittlerweile um ein Vielfaches grösser als der weltweite Drogenhandel. Ich sage, es ist einfacher und mit weniger Risiken verbunden, irgendwo aus Sibirien heraus einen Hackerangriff zu starten, als mit einem verschluckten Drogenpäckchen durch den Zoll zu laufen. Die Risiken der Hacker, die solche Angriffe durchführen, sind klein und deshalb attraktiv für sie. Und es kann damit viel Geld verdient werden.

Warum ist das Risiko für die Hacker nicht sehr gross?

Als Beispiel ist Ransomeware als ganz normales und gutes Geschäftsmodell zu betrachten. Ich verschicke ein paar Millionen Mails, irgendeiner wird auf den Link klicken und den Trojaner herunterladen. Die Daten des Opfers werden dann verschlüsselt. Auf Grund der Daten findet der Hacker sehr schnell heraus, wie hoch er seinen Preis ansetzen muss, der dafür bezahlt wird. Im Darknet existieren Firmen, die den optimalen Preis, der höchstwahrscheinlich bezahlt wird, analysieren.

Ein Drittel der Schweizer KMU hat in den letzten zwei Jahren einen Angriff auf die IT-Infrastruktur oder ähnliche Vorfälle erlebt, ergab eine Umfrage der FHNW.

Die Anzahl der ernst zu nehmenden Angriffe wird nicht abnehmen, sondern eher zunehmen. Das heisst, wir müssen lernen, damit zu leben.

Wenn wir einen Auftrag von einer Firma erhalten, sie anzugreifen, kommen wir immer rein. Immer. Aber die meisten Firmen bemerken es gar nicht, dass wir in ihr Netzwerk eingedrungen sind. Die Erkennung von Angriffen ist heute eine der wichtigsten Disziplinen geworden. Das bedeutet, man merkt, wenn ein Unberechtigter im —//

Zur Person

Marco Marchesi (49) war 1999 einer der Gründer der Firma ISPIN. 2018 wurde ISPIN mit dem Ziel einer weiteren Expansion in der Schweiz und in Europa in die CymbiQ Group integriert. In den letzten drei Jahren hat Marco Marchesi mit seinem Team die Kompetenzen der Gruppe Schritt für Schritt ausgebaut. Dabei wurden der Hosting-Anbieter Aspectra AG, der österreichische Managed Security Service Provider Anovis sowie die Winterthurer Koch-IT, eine Softwareentwicklungsfirma für hochsichere Anwendungen, in der CymbiQ Group zusammengeführt.
Seit dem 15. April 2021 konzentriert sich der diplomierte Elektro- und Wirtschaftsingenieur HTL und Vorstand des Branchenvereins Digitalswitzerland als Verwaltungsratspräsident der CymbiQ darauf, die laufenden Wachstumsschritte der Gruppe erfolgreich umzusetzen und die weitere Internationalisierung der Gruppe strategisch voranzutreiben.
www.ispin.ch / *www.cymbiq.group* / *www.digitalswitzerland.com*

Firmennetzwerk ist. Im Ruag-Fall zum Beispiel, dauerte es über ein Jahr, bis es aufgefallen ist. Im Durchschnitt befindet sich der Angreifer etwa 200 Tage im Netz, bevor der Angriff schlussendlich durchgeführt wird. Das heisst, das Erkennen der Angreifer hat eine ganz andere Bedeutung erhalten, als noch vor ein paar Jahren. Die meisten KMU sind nicht darauf ausgelegt, einen Angriff zu bemerken. Und wenn man nicht darauf ausgelegt ist, kann man fast nichts dagegen machen. Es wird so sein, dass KMU lernen müssen, nicht nur den neuesten Server einzukaufen, sondern auch den Detection-Service. Angeboten werden diese Services unter dem Namen MDR-Services, Managed Detection & Response Services.

Betrifft das eher die grösseren KMU?

Nein, es sind auch kleinere davon betroffen. Die Griesser Storen AG ist so ein Fall. Zufällig hätte der Monteur einen Tag nach dem Vorfall bei mir zu Hause vorbeikommen sollen, um neue Storen zu montieren. Jemand von Griesser hat mich dann angerufen und gesagt, sie wüssten nicht, ob sie vorbeikommen könnten, da sie nicht sagen können, ob das Produkt für uns bereitsteht. Auch dieses Beispiel zeigt die starke Abhängigkeit von digitalen Systemen. Jedes KMU kann Opfer einer solchen Attacke werden, wenn es sich nicht sorgfältig vorbereitet und schützt.

Sollte eine Firma offen kommunizieren, wenn sie angegriffen wurde, wie beispielsweise der Haustechnik-Anbieter Meier Tobler?

Ich finde es gut, wenn ein Vorfall offen kommuniziert wird. Ich behaupte, dass auch der Imageschaden heute nicht mehr so gross ist, wenn eine Firma angegriffen wurde.

Gemäss dem Motto: Das kann jedem passieren?

Ja, genau. Mittlerweile ist es bekannt, dass unzählige Firmen davon betroffen sind. Es finden Hunderte von Angriffen in der Schweiz statt. Der Schaden entsteht dadurch, dass ich meine Ware nicht produzieren, verkaufen oder liefern kann. Wichtig ist es, im Rahmen einer Krisenkommunikation alle Kunden zu informieren.

Und gutes Krisenmanagement muss vorbereitet werden. Ein KMU kann dabei pragmatisch vorgehen, die Szenarien müssen einfach einmal klar durchgedacht werden. Man muss an das denken, was wehtun könnte – auch wenn man das vielleicht nicht ohne weiteres macht. Der Mensch verschliesst sich gern ein bisschen davor.

Wer ist in den Firmen verantwortlich für die IT- und Cybersicherheit? Ist das Chefsache?

Eigentlich ist es eine der Aufgaben des Verwaltungsrats. Vom Gesetz her ist er verpflichtet, die Kontinuität des Geschäfts sicherzustellen, dazu gehört die Notfallvorsorge.

«Die meisten KMU sind nicht darauf ausgelegt, einen Angriff zu bemerken.»

Das Thema Business Continuity ist nicht nur in der Schweiz, sondern in den meisten Ländern gesetzlich vorgeschrieben. Die Umsetzung wird mehrheitlich in der IT oder in der Security vollzogen. Auch hier kann mit einem externen Partner zusammengearbeitet werden. Manchmal wird das Projekt dann aber von der Chefetage wieder zurückgestellt, weil man andere Prioritäten hat.

Muss man sich Sicherheit leisten können?

Ja und Nein. Die Frage ist eher: Kann ich es mir leisten, nicht in die Sicherheit zu investieren. Es ist immer auch ein Abwägen zwischen Sicherheit, finanziellem Aufwand und der Machbarkeit. Ich muss das Thema so aufstellen, dass meine Mitarbeitenden es auch anwenden. Wenn ich einen derart hohen Sicherheitsanspruch habe und meine Mitarbeitenden haben dadurch einen hohen Aufwand, dann werden sie meine Vorgaben umgehen. Es braucht eine Balance zwischen Wirtschaftlichkeit, Sicherheit und Anwendbarkeit. Das ist ein wichtiger Punkt, gerade im KMU-Umfeld. Für ein KMU ist es schwieriger, das ist sicherlich so. Auch hier kommen immer mehr Managed-Service-Angebote auf den Markt.

Wie sieht es mit der Sicherheit bei einem Smart Home aus?

Dort meine ich, dass es genau das Gleiche ist, wie bei einem KMU. Hier sollten aber die IT-Provider zusätzlich eine entsprechende Cyber-Defense-Lösung anbieten.

Dann sollten also auch die Hersteller der Software für Smart Home die Sicherheit bereits im Produktangebot integrieren?

Ja, das ist so. Das müsste man voraussetzen. Dazu haben wir gewisse Konzepte mit der Firma ISPIN bereits angedacht. Eine Möglichkeit wäre, dass die Hersteller oder Provider von Smart-Home-Lösungen auch noch einen Managed-Response-Service anbieten, der in dem Haus läuft.

Das gibt es noch nicht?

Das gibt es aktuell noch nicht. Es würde Lösungen geben, diese müssten aber erst realisiert werden. Und damit sind wir bei der finanziellen Thematik, da es individuelle Lösungen wären. Wenn ich ein schönes Haus baue, dann kostet das auch eine Menge Geld. Und dann würde es sich wahrscheinlich auch lohnen, eine richtige Smart-Home-Lösung zu implementieren.

Auch bei der Cloud gibt es manchmal Fragezeichen, vor allem, wenn mehrere auch im Ausland benutzt werden. Aktuell möchte der Bund seine Public Cloud von einem chinesischen Anbieter realisieren lassen.

Im Bundesumfeld würde ich sehr stark darauf achten, dass die Datenhoheit in der Schweiz bleibt. Wir müssen kontrollieren können, wohin die Datenflüsse gehen und wen es betrifft. Aus diesem Grund haben Schweizer Datencenter den Vorteil, wie die Aspectra AG in unserer Firmengruppe, dass wir ganz genau wissen, was auf unseren Servern passiert. Das ist eine Seite der Betrachtungsweise. Auf der anderen steht die Frage, ob mein PC zuhause sicher ist oder die Daten in der Cloud eines professionellen Anbieters besser aufgehoben wären. Deshalb kann die Cloud in der Zwischenzeit die sicherere Variante sein, da auch die entsprechenden Sicherheitslösungen dazu vorhanden sind.

Inwiefern ist bei der Wahl einer Cloud-Lösung der Preis ausschlaggebend?

Dazu muss man immer eine komplette Betrachtungsweise anwenden. Mit was zahle ich wirklich? Einen Teil zahle ich über den Preis, einen Teil zahle ich mit meinen Daten. Deshalb ist der Preis günstig. Aber im Gesamten ist es dann vielleicht nicht günstig, und zwar in dem Moment, in dem die Daten nicht mehr sicher sind. Dann wird der Preis plötzlich sehr hoch.

Wenn es das Smart Home gewisser exponierter Personen betrifft, dann muss man genau überlegen, was man dort einbaut. Ich wäre da sehr restriktiv und ganz vorsichtig. Ich verwende beispielsweise einen Handvenenscanner, und die Zutrittssysteme befinden sich nicht im Netz. Vom Chaos Computer Club wurde ein europäischer Flughafen bereits vor Jahren mit einem «Tag der offenen Tür» überrascht. Darauf musste man den Flughafen evakuieren, weil man nicht mehr wusste, wer drinnen und wer draussen sein sollte. Das Zutrittssystem und das Alarmsystem wurden deshalb abgehängt, die Kameras wurden nicht via WLAN mit dem Leitsystem verbunden, sondern mit einem Kabel. Das WLAN kann gestört und damit die Kameras abgeschaltet werden. Deshalb sollten die Netzwerke komplett getrennt werden, was oft unterlassen wird.

Sind nicht nur Fachleute aus der Branche, sondern auch Anbieter mit dem Thema Sicherheit überfordert?

Ich bin der Meinung, dass in Zukunft Firmen entstehen werden, die das ganze Thema IT im Gebäude, nicht von der Seite Elektrotechnik herkommend, sondern von der IT oder der Softwareentwicklung, abdecken können. Eigentlich sind für die Gebäudeleitsysteme Softwareentwickler notwendig. Es ist eine andere Denkweise, die für diese Aufgaben erforderlich ist. Das sehe ich auch bei uns in der IT-Branche. Wenn ich Mitarbeitende für die Infrastruktur mit denen für die Softwareentwicklung vergleiche, dann sind beide komplett anders. Beide haben einen völlig unterschiedlichen Ansatz mit völlig unterschiedlichen Lösungen.

Auch wenn sich der Elektroinstallateur mit einer Weiterbildung IT-Kenntnisse aneignen würde?

Ja, denn es sind völlig verschiedene Charaktere, die in den beiden Disziplinen tätig sind. Eigentlich sollten die Elektriker und Softwareentwickler in einem Team zusammenarbeiten.

Hat die Pandemie die Angriffswellen von Hackern verstärkt? Wurde durch die Homeoffice-Pflicht die IT-Sicherheit reduziert?

Am Anfang der Pandemie wurde eine starke Zunahme der Angriffe registriert. Es gibt Studien, die zeigen, dass die Angriffe um mehr als die Hälfte zugenommen haben. Viele Firmen waren nicht auf diese Situation vorbereitet. Wenn man vom Discounter dann ein Notebook kauft, selber installiert, so ist meistens die Cybersicherheit nicht gegeben. Mit dem Resultat: Alles ist offen. Und genau dort wird jetzt angegriffen. Wenn der PC angegriffen wird, gibt es zwei Möglichkeiten. Zum einen kann man von dort auch durch einen gesicherten Zugang in das Firmennetzwerk gelangen, wo die Person arbeitet. Zum anderen können in dem Heimnetz noch andere Sachen angegriffen werden. Die Angreifer —//

«Die Cyber-Crime-Branche ist eine professionell funktionierende Industrie.»

setzen sich auf ein IT-Device und schauen, was sich so alles anbietet, und dann gehen sie zum nächsten Device.

Die könnten auch auf das Smart-Home-Netz zugreifen?

Ja, am besten vom Switch der Kaffeemaschine aus, den niemanden interessiert.

Ist das jetzt ein Plädoyer für die Rückkehr ins Büro?

Die Büroinfrastruktur ist meistens besser abgesichert. Als Firma muss man Geld investieren, um das Thema Homeoffice und Endpoint-Detection und Protection richtig anzugehen. Das ist zwingend. Viele Firmen sind von der Pandemie überrascht worden, zudem musste das Geschäft am Laufen gehalten werden. Damit ist man gewisse Risiken eingegangen, für die einen hat es sich ausgezahlt, für die anderen nicht.

Wird es allenfalls auch zu Spätfolgen kommen?

Wenn der Angreifer drin ist, wartet er und schläft. Die meisten Fälle, über die wir in der Zeitung lesen, stammen von vor zwei Jahren. In dem Sinne ist es auch ein Massengeschäft, der Angreifer kann warten. Auf der Hackerseite gibt es spezialisierte Firmen, die attackieren und sagen, ich bin dann mal drin. Ich verkaufe den Zugang. Dann gibt es eine andere Firma, die schneidert einen Trojaner auf Mass, und dann führt eine dritte Firma den Angriff aus. Das sind alles hochspezialisierte Firmen in der Cyber-Crime-Branche. Diese Branche ist alles andere als eine Pionierindustrie. Es ist eine hochprofessionelle, völlig ökonomisch funktionierende Industrie, wie jede andere auch.

Existiert ein grosser Konkurrenzkampf bei den Anbietern von IT-Security?

Ja, es gibt Konkurrenz. Es war ein unheimlich fragmentierter Markt, der seit etwa 4 Jahren am Konsolidieren ist.

Firmen schliessen sich zusammen?

Das Thema Cyber Security ist zwar mit einem Wort beschrieben, inhaltlich ist es jedoch sehr komplex geworden. Damit ich als Firma die richtige Breite thematisch abdecken kann, muss ich mindestens 200 Mitarbeitende haben. Darum war es absehbar, dass sich der Markt irgendwann konsolidieren wird. Das war auch ein Grund, warum ich mich mit der Firma ISPIN bereits 2015 mit dem Gedanken beschäftigt habe. 2018 habe ich dann, zusammen mit einer Kapitalgesellschaft, die CymbiQ Group gegründet. Mittlerweile haben wir drei Firmen dazugekauft, weitere werden noch dazukommen.

Die CymbiQ Group bewegt sich auch im europäischen Markt?

Ja, unser Fokus ist DACH. Aber auch die nordischen Länder sind für uns interessant, sie sind uns von der Kultur her sehr nah.

Wie ist die Schweiz grundsätzlich bei der Cyber Security aufgestellt?

Die Schweiz hat auch auf Bundesebene mittlerweile einen sehr guten Job gemacht.

Es sind der Cyber Defense Campus und das nationale Cybersicherheitszentrum entstanden, zudem wurden auch die dazugehörenden Ressourcen gesprochen. Ebenfalls wurde eine Eidgenössisch anerkannte Ausbildung als Cyber-Security-Spezialist geschaffen, die man im Rahmen der RS absolvieren kann. Das war eine Zusammenarbeit von Wirtschaft, Bund und Armee – so etwas geht nur in der Schweiz, das ist sehr bemerkenswert. Wir sind allerdings nicht fertig und müssen uns kontinuierlich verbessern.

Die Entwicklungen verlaufen sehr schnell, wobei die Pandemie zum Teil grundlegende Veränderungen mit sich gebracht hat. Für Cloud-Lösungen müssen die Sicherheitskonzepte völlig anders aussehen. Heute arbeiten Firmen mit Hunderten von Clouds. So spielt es eigentlich keine Rolle mehr, ob ich innerhalb eines Firmennetzes bin oder in einem Co-Working-Space sitze. Den Perimeter einer Firma gibt es nicht mehr, deshalb muss das Sicherheitskonzept anders aufgestellt sein.

Heute geht es nur noch darum, die sogenannte Zero-Trust-Architektur anzuwenden. Das heisst, ich traue keinem Umfeld mehr, in dem ich mich befinde. Deshalb ist es auch egal, wo ich bin.

Könnten Sie zum Schluss noch Ratschläge an Unternehmen geben, wie sie mit den digitalen Risiken umgehen sollen?

Grundsätzlich sollte das Thema IT- und Cybersicherheit ganz oben auf der Agenda stehen. Bei jedem Projekt, das man macht. Die alte Denkweise, dass man nicht interessant genug ist, um angegriffen zu werden, muss auf die Seite gelegt werden. Jeder ist interessant.

Und man sollte auch einmal eine gewisse Summe investieren, um einen Service einzukaufen oder eine Beratung von einem externen Spezialisten. Die Thematik ist zu komplex und verlangt nach speziellem Wissen. Darum ist das Thema Managed Service auch für Sicherheit, nicht nur für IT, ein ganz wesentlicher Punkt und muss zwingend bei jedem Digitalisierungs-projekt unabdingbarer Bestandteil sein. —▭