BRAUCHT ES EINE CYBER FEUERWEHR? SWISS BUSINESS PROTECTION AG

INTERVIEW MIT CHRIS ECKERT (CEO) UND WOLFGANG SIDLER (STV. CEO)

INTERVIEW VON CHRISTOPH BORER

1 Swiss Business Protection AG wurde im vergangenen Juli gegründet. Was ist das Kernziel, das Sie erreichen wollen?
Die Wirtschaft in der Schweiz, namentlich unsere Unternehmen, Institutionen sowie auch Private sollen unbürokratisch und wirksam gegen die aktuellen und künftigen Gefahren im Bereich Wirtschaftskriminalität, Cyber Crime und Industriespionage geschützt werden. Mit acht Expertinnen und Experten sowie ihren Firmen – alle seit Jahren in den verschiedensten Bereichen der Integralen Sicherheit tätig – werden Geschädigte, Hilfesuchende und Betroffene unterstützt. Im Ernstfall begleiten wir sie mit allen erforderlichen Massnahmen, bis der Normalfall wieder eintritt oder die Krise überwunden ist. Gesamtheitlich, zeitnah, vertraulich und aus einer Hand. Konzeptionell, strategisch und operativ. Sieben Tage die Woche. Im Notfall auch am Wochenende und in der Nacht. Ende Oktober 2019 wurde das Kompetenzzentrum Wirtschaftsschutz Schweiz (Swiss Business Protection AG; *www.swissbp.ch*) offiziell eröffnet.

2 Das Thema Cybercrime und Cyber-Security ist in der heutigen Zeit ein Thema, das immer mehr im Focus der Unternehmen steht weil das Thema immer mehr ein Geschäft wird. Wie sehen Sie die Entwicklung?
Die Gefährdungslage für unsere Wirtschaft ist bereits heute auf einem hohen Niveau. Die Zahl der Cyberattacken auf Industrie- und Dienstleistungs-Unternehmen wird wohl auch künftig weiter steigen. Parallel dazu wird die Qualität der Angriffe ebenfalls neue Dimensionen erreichen. Immer mehr Daten, Informationen und sensible Dokumente werden künftig in digitaler Form örtlich und zeitlich unabhängig voneinander abrufbar sein. Schneller verfügbar, effizienter einsetzbar und einfacher bedienbar heissen die Ansprüche des heutigen Anwenders. Diese Entwicklung ist aus Sicht der Usability toll, ergibt aber seitens der Integralen Sicherheit immer mehr offene Einfallstore und grössere Angriffsvektoren für Attacken, digitale sowie konventionelle.

Derzeit werden zum Beispiel Trojaner meistens als Spam- und Phishing-E-Mail verschickt, welche Dateien und Programme durchsuchen und schliesslich weitere Malware nachlädt, welche die Kontozugangsdaten abfischen. Danach kommen die Verschlüsselungs-Trojaner ins Spiel: Sie verschlüsseln wichtige Dateien und fordern die Geschädigten auf, Lösegeld z.B. in Bitcoins zu bezahlen.

In dieser ganzen Phase sind wir alle, also der normale Anwender, im Spiel. Mindestens vor jedem Cyberangriff wird durch die Täter Social Engineering betrieben. Die grösste Schwachstelle ist leider der «Risikofaktor Mensch» also der Benutzer am Computer, welcher z.B. das Phishing-E-Mail öffnet. Wir Menschen treffen zum überwiegenden Teil emotionale Entscheidungen (Gutmütigkeit, Hilfsbereitschaft, Angst, Mitleid, Vertrauen). Das macht uns verletzlich und angreifbar. Hacker, Kriminelle etc. nützen dies schamlos aus. Beim vorgenannten Beispiel wird der Anwender mittels Manipulation oder Ablenkung dazu bewegt, den Anhang im E-Mail zu öffnen.

Und die nahe Zukunft zeigt keine Abkehr: Die Anbindung von Produktionssystemen ans Internet (IoT) und der Einsatz von Cloud-Diensten verspricht im Zuge der Digitalisierung und der Industrie 4.0 mehr Effizienz und Produktivität in den Unternehmen. Jedoch bieten zusätzliche digitale Komponenten und Cloud-Services eine deutlich höhere Anzahl von Schwachstellen und Angriffsmöglichkeiten für Hacker und kriminelle Organisationen.

3 Was mir auch auffällt, dass die Aufklärungsquote von Cyberangriffen in vielen Ländern sehr tief ist. Kann man sagen, dass die Justiz dieser Thematik einfach nicht gewachsen ist?
Diese Frage kann seriös nicht mit einem Einzeiler beantwortet werden. Grundsätzlich wird nach einem Vorfall nur ein Bruchteil der Angriffe den Strafverfolgungsbehörden gemeldet, also eine Strafanzeige erstattet. Dies hat verschiedene Gründe: Der betroffene Unternehmer beispielsweise möchte in erster Linie möglichst schnell die negative Einwirkung stoppen, den Schaden begrenzen, die Produktion möglichst schnell wieder hochfahren und tunlichst einen Reputationsschaden vermeiden. Die Strafverfolgung eines identifizierten Täters ist für ihn nur ein nachgelagertes Ziel. Bei den Strafverfolgungsbehörden ist es genau umgekehrt. Polizei und Staatsanwaltschaften haben den gesetzlichen Auftrag, Straftaten zu verfolgen, Täter zu ermitteln, gerichtsverwertbare Beweise zu erheben, um die identifizierte Täterschaft später durch ein Gericht bestrafen zu lassen. Ob dann eine betroffene Firma im schlimmsten Fall z.B. keine finanziellen Reserven mehr hat, um mit eigener Kraft wieder hoch zu kommen, ist nicht Sache und Verpflichtung des Staates. Dazu kommt, dass Cyber-Kriminelle und kriminellen Organisationen meist abgeschottet im Ausland oder mobil sind, von dort aus punktgenau agieren und kaum strafrechtlich verfolgt werden können. Dazu wäre eine sehr grosse Anzahl von Ermittlern, IT-Spezialisten, Elektronikern, Forensikern, Hackern und spezialisierten Staatsanwälten erforderlich, was wiederum massive Kosten verursachen und ein völlig neues, unbürokratisches Vorgehen und pragmatische Gesetzgebung voraussetzen würde. Die teils sehr langsame grenzüberschreitendet Zusammenarbeit sowie eine Strafverfolgung, welche auf länderspezifischen, unterschiedlichen gesetzlichen Bestimmungen basiert ist aber die Realität. Dies rasch zu optimieren und zu verbessern, ist unseres Erachtens ein Wunschtraum. Die Wirtschaft muss also selbst für ihren Schutz sorgen. Warten auf eine übergeordnete Lösung ist nicht zielführend.

4 Das Thema Cyber-Angriffe ist kein neues Phänomen sondern das Problem gibt es schon ein paar Jahrzehnte – ich kann mich noch an einen bösartigen Virus erinnern, MYDoom, im Jahr 2001. Das zeigt mir, dass das Thema eigentlich jahrelang nicht beachtet wurde?
Ihre Einschätzung ist richtig. Schon in den 80er Jahren gab es zuhauf Erpressungs-Faxmeldungen z.B. aus Nigeria mit dem Ziel, sich auf unsere Kosten zu bereichern. «Sie haben gewonnen!» oder «Lukrativer Nebenverdienst!» – hinter solchen Angeboten steckten und stecken oft Betrüger und Abzocker. Oder denken Sie an den alt bewährten Enkel-Trick. Der wird heute noch erfolgreich angewandt. Sie sehen, die Täter sind kreativ, passen sich schnell den Gegebenheiten an und setzen einfach sowie günstig verfügbare Technik und Elektronik erfolgreich ein. Auch hier zeigt sich, dass der «Mensch» ziemlich einfach angreifbar ist.

Uns Menschen hier geht es gut. Wir sehen meist nur das Positive und blenden dadurch gewisse Gefahren oder Risiken aus. Zudem machen wir uns erst ernsthafte Gedanken, wenn man selbst oder direkt negativ betroffen ist. Es muss also zuerst schmerzen, bis wir reagieren. Die Materie ist teils zu abstrakt, physisch nicht fassbar und schon gar nicht sichtbar. Also weshalb soll ich mich gegen etwas schützen, was ich nicht kenne und noch nicht eingetreten ist?

Unser Ziel ist es, die Menschen bzw. die Unternehmen in dieser Hinsicht aufzuklären und zu sensibilisieren. Das heisst, präventive organisatorische und technische Massnahmen zu treffen um einen möglichen Angriff erfolgreich zu überstehen oder es gar nicht so weit kommen zu lassen. Kommt es zu einem Angriff, unterstützen wir die Unternehmen von Anfang an bis zum Schluss, um die richtigen Entscheidungen zu treffen, den Schaden zu minimieren und baldmöglichst den Normalbetrieb wieder zu ermöglichen.

5 Viele Unternehmen haben der Problematik bis heute auch keine Beachtung geschenkt. Kann man sagen, dass das Risiko einer Cyber-Attacke von vielen Unternehmern ignoriert worden ist?
Wir sollten den Fokus nicht nur auf Cyber-Attacken legen. Die erweiterte Betrachtungsweise schliesst z.B. auch Industriespionage, Sabotage und Wirtschaftskriminalität mit ein. Dies sind ebenso grosse Bedrohungsfelder, die meist nicht losgelöst voneinander einwirken. Das macht die Erkennung und Identifikation eines Vorfalls oder Schadens nicht einfacher.

Wir hören noch oft von Verantwortlichen «davon sind wir nicht betroffen» oder «das passiert uns nicht, denn wir sind ja kein Rüstungskonzern». «Sicherheit kostet nur» ist eine weitere Argumentation. Das heisst, die Unternehmen «fühlen» sich sicher, wissen es aber letztlich nicht wirklich. Das ist eine gefühlte Sicherheit, man könnte eine solche Haltung in der heutigen Zeit auch als Ignoranz bezeichnen.

Das Ziel einer Unternehmensführung sollte unseres Erachtens sein, u.a. die eigenen Mitarbeitenden zu schützen, eine reibungslose Produktion zu gewährleisten und die Verfügbarkeit von Information sowie Innovation zu sichern, um die Prosperität des Unternehmens auch in Zukunft zu gewährleisten. Der Schutz der zentralen Unternehmenswerte eines jeden Unternehmens ist das prioritäre Interesse. Die Einbettung einer integralen Sicherheit in die Geschäftsstrategie tut Not.

Wir können jedem Unternehmen nur empfehlen mindestens eine Risiko-Analyse, speziell auf das eigene Unternehmen ausgerichtet, durchzuführen.

6 Heutzutage kann man bei Hackern Tools kaufen, die man für Cyber-Attacken einsetzen kann und falls man mit dem Tool nicht zurecht kommt steht einem sogar ein Help-Chat zur Verfügung. Das sagt mir, es geht wie immer nur ums Geld. Braucht es eine Cyber-Polizei?
In der Tat gibt es solche Dienstleistungen, z.B. «Hacking-as-a-Service». Vollständige Angriffspakete inkl. 24Std. Hotline können Sie im Darknet kaufen. Da die Kriminellen inzwischen erkannt haben, dass sie selbst das Know-how nicht mehr haben müssen um beispielsweis mit Phishing-Attacken sehr viel Geld zu verdienen, wurde dies zu einem sehr erfolgreichen Business-Modell.

Der Ruf nach einer Cyber-Polizei ist verständlich. Aus schon erwähnten Gründen sind wir bezüglich effektiver Wirkung auf internationaler Ebene skeptisch. Mit unseren demokratisch austarierten Gesetzen, den unterschiedlichen Interessen der einzelnen Länder und dem Ruf nach differenziertem Einsatz der Steuergelder können wir im Bereich der Bekämpfung wohl einzelne Organisationen identifizieren, nur ein paar Täter dingfest bzw. inaktiv machen. In der Schweiz gibt es Spezialisten in den Polizeikorps, die sich der Verbrechensbekämpfung im Cyber-Bereich annehmen. Ein gezielter Ausbau wäre aus unserer Sicht zweifelsfrei nötig. Letztlich kann aber die Wirtschaft nicht tatenlos zusehen und auf Besserung hoffen. Die Zeit rennt uns buchstäblich davon.

7 Ein wichtiger Punkt zum Schutz vor Cyber-Attacken ist die Aufklärung und Schulung von Mitarbeitenden?
Das ist genau der Ansatz. Die Mitarbeitenden sollten regelmässig zum Thema der Integralen Sicherheit sensibilisiert werden. Es nützt nichts, nur einmal mit einem internen E-Mail über Cyber-Risiken zu informieren. Awareness und Sensibilisierung ist ein permanenter Prozess. Es gibt viele praxisorientierte Sensibilisierungs-Massnahmen. Ein gutes Awareness-Konzept mit entsprechenden Massnahmen ist ein sehr wichtiger Beitrag für die Sicherheit Ihres Unternehmens. Sicherheit ist zur Chefsache geworden. Die obersten Chefs tragen die Verantwortung. Und letztlich haftet der Verwaltungsrat.

8 Swiss Business Protection AG wirbt mit dem Slogan «Wir schützen Ihr Unternehmen». Wie muss ich mir das vorstellen?
Wir schützen Unternehmen mit dem integralen Sicherheitsansatz:

Prävention (proaktive Dienstleistungen):
Selbstverständlich ist der beste Schutz des Unternehmens gewährleistet, wenn negative Einwirkungen oder Angriffe verhindert werden können. Im besten Fall werden mit wiederkehrenden, präventiven Massnahmen Risikobeurteilungen durchgeführt, Sicherheitsstrategien entwickelt, Awareness- und Sensibilisierungskampagnen implementiert sowie mit wiederkehrendem Controlling (z.B. Audits) überprüft und aufgrund der aktuellen Erkenntnisse angepasst.

Basierend auf den drei Säulen eines jeden Unternehmens (Infrastruktur, Mensch & Organisation sowie Information) gilt es – je nach Ausgangslage und Ausrichtung des jeweiligen Unternehmens – Überlegungen zu Aspekten wie Standortsicherheit, Risikofaktor Mensch, Rekrutierung, Mobilitätssicherheit, Notfall- und Krisenmanagement, Forensik, Know-how-Schutz sowie Cyber Security bzw. generellem Informations- und Datenschutz anzustellen und gezielte Abwehr- und Gegenmassnahmen umzusetzen.

Ereignisbewältigung (reaktive Dienstleistungen):
Die rasche und zielgerichtete Ereignisbewältigung gewinnt ständig an Wichtigkeit. Immer wieder wird der Ruf nach einer Anlaufstelle laut, welche kontaktiert werden kann, wenn der Schaden nach einem Vorfall eingetreten ist oder die Krise kein Ende nehmen will. Der Ansatz dieser Anlaufstelle sollte sein, bei einem Vorfall möglichst schnell, angemessen und wirkungsvoll zu reagieren und das geschädigte Unternehmen oder den Betroffenen zu begleiten. Gleichzeitig wird der Wunsch nach schweizerischen oder zumindest regionalen Anbietern geäussert, die sich durch ihre operative Erfahrung, interdisziplinären Kompetenzen, gesamtheitliche Betrachtung und ihre verhältnismässig skalierbare Agilität auszeichnen müssten.

9 Wie läuft es ab wenn ich Swiss Business Protection AG kontaktiere?
Ein schadenreicher Vorfall, ein negatives Ereignis macht Sie betroffen. Oder Sie haben Bedarf für präventive Beratung im Bereich der integralen Sicherheit. Ein Anruf genügt. Ein Experte der Swiss Business Protection AG nimmt Ihr Anliegen entgegen, fragt nach und führt eine erste Einschätzung durch.

Im Krisenfall unterstützt Sie unser Experten-Team über unsere Notfall-Nummer täglich von 06:00 bis 24:00 und bietet Ihnen Lösungen, um das Ereignis optimal zu meistern und künftige Angriffe effizient abzuwehren. Wünschen Sie eine Beratung in Form der Prävention erreichen Sie uns zu den üblichen Bürozeiten. Wir begleiten Sie mit grösster Diskretion bei der Ereignisbewältigung, wie auch bei der Prävention. Von Anfang bis zum Ende und alles aus einer Hand.

CYBER SECURITY

10 Welche Lösungen kann ich erwarten?
Jede Lösung hängt von der Art des Ereignisses ab. Es sind organisatorische und technische Massnahmen je nach Fall und Angriff. Präventiv können wir Ihnen das ganze Spektrum der Integralen Sicherheit anbieten. Hier gibt es sehr viele Massnahmen um Ihr Unternehmen zu schützen. Sei es das Durchführen von Audits oder Penetration-Tests, das Erstellen von Konzepten, Richtlinien und Weisungen, das Erarbeiten von zugeschnittenen Awareness-Schulungen, Durchführen von Risiko-Analysen und Zertifizierungen bis hin zur Entwicklung von Sicherheitsstrategien.

Kann man sagen Sie sind die Cyber-Feuerwehr der Schweiz?
Die Analogie kommt hin, aber nicht nur im Bereich von Cyber-Attacken. Die Feuerwehr ruft man erst, wenn das Ereignis bereits stattgefunden hat und wir mit unseren Lösungen versuchen den Schaden so schnell wie möglich einzudämmen. Wir verfügen nicht über Löschwasser, dafür aber über viel Erfahrung, aktuelles Wissen und umfangreiche Kompetenzen.

12. und letzte Frage. Wie sehen Sie das aktuelle Interesse der Schweizer Unternehmer am Thema Cyber-Security?
Bei Gesprächen auf dem C-Level ist das Thema leider noch nicht ganz angekommen. Das wird vermutlich noch einige Zeit andauern. Eine aktuelle Umfrage hat dies leider wieder bestätigt: 64% der Geschäftsleitungen sind immer noch der Ansicht, dass die Verantwortung für Cyber-Sicherheit bei der IT liegt. Dies ist ein grosser Trugschluss. Verantwortlich für das was getan und verursacht wird oder passiert, ist immer die Geschäftsleitung. Wie schon erwähnt, Sicherheit ist Chefsache!