Fridel Rickenbacher ist Mitbegründer, Partner, Geschäftsführer und Verwaltungsrat der MIT-GROUP, eines Totalunternehmens für «Empowering for the 4th Industrial Revolution» und Informations- und Kommunikationsmanagement. Auf Bundesebene ist er als Experte und Akteur vertreten bei «Digital Dialog Schweiz» + «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS». Er ist in seiner Mission «sh@re to evolve» seit

CyberCrime – nächste Wellen von Mehrfach-Erpressung und «Deep Fake»

Beitrag von Fridel Rickenbacher

Bekanntlich hatte auch das dunkle Business Modell CyberCrime in den letzten 2 Jahren von mehreren, mitunter parallel zur Covid-Pandemie verlaufenden Wellen leider wiederum massive Zuwächse und Erfolge verzeichnet.

Die Covid-Pandemie hat vieles verändert und erzwungen – auch die Digital Transformation

Viele Organisationen haben einerseits grosse Fortschritte realisieren können (müssen) zugunsten der möglichst optimierten Angriffs- und Betriebs-Sicherheit in der Dynamik der professionell organisierten Cybercrime-Akteure und andererseits auch im Bereich der forcierten Transformation in eine zunehmend digital unterstützte und effizienzsteigernden Arbeitsmethodik / Mindset im z.B. Home Office, Team Zusammenarbeit, geräte- und standort-unabhängiges mobiles Arbeiten oder auch mittels Automatisation generell.

Die System- und Services-Abhängigkeit und angepasste Planungs-Notwendigkeit nimmt weiter zu

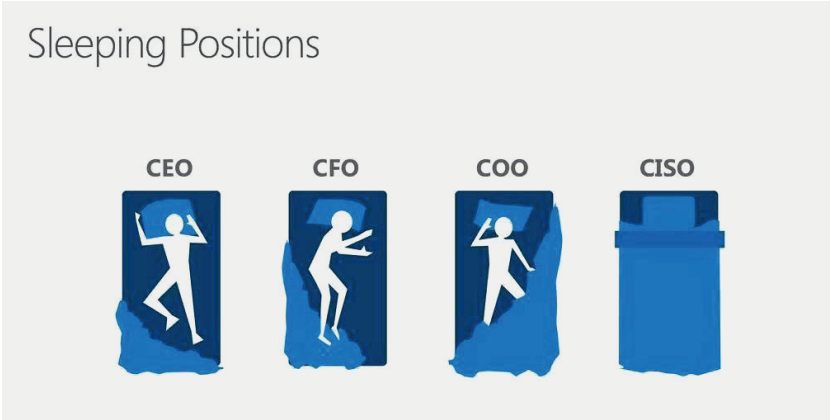
Der business-relevante und business-kritische Anteil der eingesetzten Systeme, Services, Schnittstellen, Verbindungen, Apps hat weiter stark zugenommen. Dies hat auch Auswirkungen auf die entsprechende Planung und Massnahmen gegen Ausfälle oder Angriffe im Rahmen eines sogenanntem «Business Contingency Planning» oder «Incident Response Management». In einer solchen Planung – auch als Erweiterung des «Risk Management» – ist möglichst gut zu inventarisieren, klassifizieren, schützen, abbilden, planen mit welchen organisatorischen oder technischen Massnahmen eine solche Systemabhängigkeit je nach Ausfall, Vorfall oder Angriff organisiert, optimiert, kommuniziert, überbrückt und letztlich möglichst bewältigt werden kann. Ein planloser und orientierungsloser Zustand ohne entsprechende organisatorische oder technische Vorkehrungen kann mitunter als fahrlässig betrachtet werden. Auch Versicherungen und auch spezialisierte Cybersecurity-Versicherungen haben aufgrund der dynamischen Bedrohungslage und bedrohlichen Weiterentwicklungen der Cybercrime-Akteure diverse Vorbehalte, Abmahnungen oder auch vorsorgliche Erneuerungs-Kündigungen verständlicherweise initiieren müssen.

Challenges und neue schwieriger werdende Hausaufgaben in nächster Zeit

Im Bereich des gefürchteten und leider sehr erfolgreichen Angriffs-Vektors «Erpressungs-Software» (ransomware) / «Verschlüsselungs-Trojaner» (cryptotraojaner) gibt es bedenkliche, sich negativ auswirkende Innovationen. Wo früher Daten oder Software «nur» verschlüsselt und dadurch unbrauchbar wurden, ist schon länger diese Erpressungs-Taktik sehr erfolgreich weiterentwickelt worden, in eine «doppelte Erpressung» (double extortion) mittels zusätzlich entwenden und gar angedrohtem veröffentlichen der gestohlenen Daten zur Erhöhung der Erfolgsquote der Erpressungsversuchs.
Leider ist bereits auch die «dreifache Erpressung» (triple extortion) eine weitere Innovations-Stufe bei welcher solche Daten im Falle einer Nicht-Bezahlung des Erpressungsgeldes auch zum Kauf angeboten werden bzw. gar an Geschäftspartner, Mitbewerber, Kunden usw. zugänglich gemacht werden.
Dieses Beispiel lässt einem hoffentlich erahnen, dass solche klassifizierte bzw. kritische Daten, welche entwendet werden, wenigstens möglichst gut geschützt sind mittels adäquaten Massnahmen im Bereich der Datensicherheit und Datenschutz. z.B. mittels Verschlüsselung, Data Loss Prevention, Information Rights Management, Information Compliance bzw. Management und Einschränkungen im Bereich Zugang und Berechtigungen zu denselben usw.
Das relativ einfache Prinzip von «need to know» bzw. «kleinst möglichste Berechtigung oder Zugang» auf business-kritische oder personen-bezogene Daten kann hier das Schadenspotential stark mindern. Z.B. wenn «Hans Muster» angegriffen bzw. seine digital Identität missbraucht wird, er jedoch keine unnötigen Zugänge und Berechtigungen auf solche Daten hat und sein Zugang / seine Rechte bzw. seine digitale Identität entsprechend wenig sieht, wenig entwenden oder wenig anrichten kann.
Auch in nächster Zeit wird weiterhin erfolgreich «gephisht» mittels «Phishing Attacken» bzw. «Social Engineering Taktiken» und entsprechenden, immer besser gefälschten und teilweise kontextpassenden Anfragen mittels Email, Webseite, Anrufen, SMS, Mobile Messaging.
Der bereits wieder in die Jahre gekommene «digitale Enkeltrick» mit cleverer Erschleichung von personenbezogenen Daten, Kennwörter, Zugängen, firmenkritischen Informationen usw. oder manipulativer Drängung zu gefährlichen Aktionen, Zahlungen oder Zulassen von

Jahren als Redaktionsmitglied, Experten-Gruppen- und Verbands-Aktivist tätig bei z. B. SwissICT, s-i.ch, isss.ch, isaca.ch, bauen-digital.ch rund um Digitalisierung, Engineering, Clouds, ICT-Architektur, Security, Privacy, Datenschutz, Audit, Compliance, Controlling, Information Ethics, in entsprechenden Gesetzes-Vernehmlassungen und auch in Aus- und Weiterbildung (CAS, eidg. dipl.).

gefährlichen Remote-Support-Zugängen hat leider ebenfalls einiges an Weiterentwicklungen zu bieten.
Es gibt auch hier eine «dunkle Seite der Macht im Bereich der Technologie», welche sich dann mittels Künstlicher Intelligenz (KI/AI) bzw. «machine learning (ML) weiter aufmunitioniert und mittels sogenanntem «deep fake» dann mittels täuschend ähnlicher Stimme, Sprachnachrichten, Bilder, Videos eine weitere «Schreckens-Zeitalter-Dimension» des «Social Engineering» eingeläutet hat.
Das «Internet der Dinge» (IoT) bzw. einfach gesagt die «massive Interkonnektion von jedem Ding auf dieser Welt» wird erwachsen und kann nebst den riesigen positiven Potentialen jedoch auch zum «Internet der Bedrohungen» werden ohne entsprechendes präventives Management und interdisziplinärer Zusammenarbeit aller vernetzten Akteure und Hersteller in diesem riesigen Feld.
Eine solche «massive Interkonnektion» welches schon lange unser Leben, Welt, Heim, Firmen durchwächst und teilweise auch unerwünscht zu stark bzw. «datenschutz-technisch zu heikel» Daten sendet, empfängt bzw. verbindet birgt ein nicht zu unterschätzendes Potential von gezielten oder mitunter auch unmotivierten Systemüberlastungen oder Sicherheitslücken bis hin zu sogenannten «Distributed Denial of Service» (DDoS) Attacken von ganzen Industriezweigen oder Industrielieferanten bei auch entsprechenden Unterbrüchen oder Ausfällen von ganzen Internet-Hauptverbindungen oder -Regionen.
Viele Cybercrime Organisationen setzen schon länger wieder verstärkt auf «Trojanische Pferde» und habe weitere Wege gefunden, die bei vielen Organisationen verbesserte Resilenz gegen Angriffe oder Ausfälle von langer Hand strategisch geplant zu umgehen. Solche hochspezialisierte Malware, Software, Zero Day Exploit, Komponenten usw. werden dann illegal eingepflanzt und wortwörtlich mittels einem «trojanischen Pferd» eingepflanzt in die Supply Chain, Partner oder Softwareanbieter des gezielten Kunden oder gar in den ganzen Kundenkreis des Supply Chain Partners.



Durch diesen hochspezialisierten Angriffsvektor gelingt es den Cybercrime Akteuren zunehmend, mittels sozusagen der «Hintertür» (backdoor) in die Zielorganisation einzudringen weil der anzugreifenden Endkunde dem Supply Chain Partner/Softwareanbieter «vertraut» bzw. technisch mittels Schnittstellen, Verbindungen oder eben mittels Software und Software-Updates dadurch «gefährlich verbunden» ist und die eingeschleuste gefährliche Software-/Komponente/-Update nicht oder zu spät bemerkt
Das seit Jahren sehr erfolgreiche «Business Model mit den nicht gemachten Hausaufgaben» entwickelt sich rasant und erschreckend weiter. Die Cybercrime Organisationen sind zunehmend spezialisiert und nutzen ebenfalls zunehmend und erfolgreich hoch-spezialisierte Sub-Unternehmer in deren Netzwerk. Diese sehr geschickte Orchestrierung von Spezialisten und hochspezialisierten Sub-Unternehmen gründet auf ausgeklügelte Strategien und Planungen. Man darf nur hoffen, dass alle dadurch bedrohten Organisationen ebenfalls entsprechende Strategien und Planungen («Business Contingency Planning» oder «Incident Response Management») gegen diese dynamische Bedrohungslage aufbauen und laufend weiterentwickelnd gemäss «Stand der Technik»
Ein Zitat vom Jahrhundert-Kapitalist Warren Buffet sollte das treffend ermahnen und in Erinnerung rufen können:
«An idiot with a plan can beat a genius without a plan.» –> Ein Idiot mit einem Plan kann ein Genie schlagen ohne Plan»

Alles bleibt beim Alten und mitunter bei Mittätern

Letztlich bleibt alles beim Alten. Solange die Cybercrime Akteure und Organisationen mittels deren Angriffen und Erpressungen weiterhin so erfolgreich unterwegs sind und immer wieder mehr und mehr «neues» Geld erwirtschaften damit, wird diese 7×24 h-Challenge weiterhin vielen Personen deren Schlaf rauben. (auf dem Bild ist der «CISO» der sogenannte, dafür zuständige «Chief Information Security Officer»)
Solange leider viele Organisationen durch die bekannten, jedoch nicht gemachten Hausaufgaben gezwungen werden auf solche Erpressungs-Forderungen oder gefährliche Aktionen, Zahlungen, Datenverlusten, Datenschutzverletzungen usw. einzugehen, werden diese leider mitunter zu einer «speziellen Art von Mittäter». Ist das gar eine «überspitzt interpretierte» Art von «asozialem Verhalten»?