Editorial

Drei Schlaglichter und Interviews zum Stand der IT-Sicherheit von der IT-Sicherheitsmesse ITSA im Oktober 2021“

Der Bereich der IT-Sicherheit stellt für Compliance-Spezialisten ein sicherlich wichtiges Einzelthema in der Gesamtherausforderung „Einrichtung und Unterhalt eines CMS“ dar. Allerdings eben auch nur ein Thema unter vielen. Um Ihnen, werte Leserinnen und Leser der comply. einen Einblick und Überblick über den Status Quo der aktuellen IT-Sicherheitslandschaft zu vermitteln, haben wir während und kurz nach der IT-Sicherheitsmesse ITSA in Nürnberg (12.-14. Oktober) drei Interviews mit Experten entsprechender IT-Sicherheitsangebote geführt. Allen zu eigen ist, dass sie einen tendenziell kritischen, Glanz und Gloria der auf Hochglanz polierten Cybersecurity-Angebote hinterfragenden – bisweilen auch selbstkritischen Betrachtungswinkel gegenüber Technologien und Verfahren zum Schutz von Unternehmen-Assets und Unternehmens-IT-Umgebungen einnehmen.

Sprichwort: Medio flumine quaerere aquam[1]

Die ITSA selbst hat sich in zurückliegenden Jahren zum wahrscheinlich wichtigsten Branchentreffen der europäischen IT-Sicherheitsszene entwickelt. Die erste Nach-Corona-Veranstaltung im Jahr 2021 litt sichtlich noch unter den Nachwehen der Pandemie – eine nicht unerhebliche Zahl an Branchengrößen hat offenbar noch keine Genehmigung zur Ausrichtung von Messeauftritten erhalten. Die 2021er ITSA zeigte aber – was Aussteller- und Besucherzahlen anbelangte – deutliche Erholungs-Indikatoren.

Technologien, Maßnahmen und Methoden für Prävention, Detektion, Sensibilisierung & Training, Incident Handling und Forensik stagnieren auf einem ausgereift-hohen, aber wenig grundlegend neue Innovation aufzeigenden Niveau. Innerhalb der IT-Sicherheits-Industrie finden offenbar zahlreiche Konsolidierungsvorgänge hinsichtlich der Beschäftigungsverhältnisse der besten Köpfe in Entwicklung und Vertrieb statt. Entsprechend häufig sind einmal vertraut gewordenen Ansprechpartner bei den Marktgrößen nicht mehr verfügbar oder begegnen dem „ratsuchenden Besucher“ in neuer Rolle. In wie weit dies zu einer Verbesserung der Gesamt-IT-Sicherheitslage beiträgt, darf bezweifelt werden. Für Endkunden ist es schwer, ein integres Vertrauensverhältnis zu Köpfen und Ansprechpartnern bei IT-Sicherheitsausrüstern zu schaffen, wenn diese Ansprechpartner in schneller Abfolge von Arbeitgeber zu Arbeitgeber wechseln.

Von vielen Seiten beklagt wird ein fehlendes Gesamtverständnis für die tatsächlichen Gefahren aus dem Cyberraum sowie die mangelhafte Abstimmung und Zusammenarbeit unterschiedlichster Werkzeuge und Präventions-Technologien. Und es ist viel Halbwissen in der Szene anzutreffen. Eine überschaubare Zahl „echter IT-Sicherheitsexperten“ teilt sich den Vertriebsraum mit einer großen Zahl selbsterklärter Security-Spezialisten, denen allerdings häufig grundlegende Zusammenhänge und ein profundes Hintergrundwissen zur Systematik der IT-Sicherheit fehlen. Kaschiert wird dies allenthalben durch eine Flut schwer einzusortierender, oft durch Marketingspezialisten etablierter und den Benutzer darin verwirrender Fachbegriffe, Abkürzungen und Anglizismen, die - undefiniert und unerklärt in Argumentationsketten aneinandergereiht - über die Ratsuchenden ausgeschüttet werden.

[1] In der Mitte des Flusses das Wasser suchen. Wir sagen heute – „Den Wald vor lauter Bäumen nicht sehen“

Doch es gibt auch die Perlen, die Köpfe, die ein breites Basiswissen zur IT-Sicherheit mit einem kritischen, hinterfragenden, weit über die Tellerränder der eigenen Disziplin hinausschauenden Gesamtblick erfassen können, die um die Ecke denken und in bestehenden Defiziten und Unzulänglichkeiten Chancen und Innovationsnischen entdecken. Diese aufzuspüren und für Sie, unsere treuen Leserinnen und Leser zu befragen, war eines unserer Hauptanliegen beim dreitätigen -und wie so oft an diesem Ort auch beflügelnden, zahlreiche neue Ideen und Impulse vermittelnden Messebesuch. Wir haben die drei ausgewählten IT-Sicherheitsexperten jeweils mit den gleichen Interview-Fragen adressiert und geben Ihnen deren Antwort, teilweise ein wenig verkürzt und kondensiert - aber so weit als möglich im transkribierten Originalwortlaut - wieder. Wir verzichten bewusst auf jedwede Interpretationen oder Vergleiche zwischen den Antworten und wollen dies ganz gezielt Ihnen, unseren im Tagesgeschäft mit Compliance-Themen beschäftigten Leserinnen und Lesern überlassen. Viele Rückschlüsse und individuelle Erkenntnisse für Ihre Aufgaben und Herausforderungen resultierend aus den drei Stimmungsbildern zur IT-Sicherheitslage im Oktober 2021 wünscht Ihnen -Ihr Richard Huber

Interviewpartner 1: Stefan Bange (SB),

Herr Stefan Bange ist Country Director DACH beim 2013 gegründeten, europäischen Sicherheitsunternehmen CybelAngel mit Hauptsitz in Paris und dabei verantwortlich für den strategischen Aufbau der DACH Region. Das Unternehmen ist weltweit aktiv im Bereich der „Data Breach Prevention [2]sowie Asset Discovery & Monitoring[3]“ und betreut dabei vorwiegend große mittelständische Unternehmen ab ca. 500 Mitarbeitern sowie Großkunden – auch multinational - aus der freien Wirtschaft. Herr Bange ist seit 15 Jahren in der Softwareindustrie und in der Informationssicherheit in Managementpositionen unterschiedlicher Unternehmen in Aufbau- und Skalierungsphasen unterwegs. Seinen ersten Computer bekam er mit 6 Jahren und seither ist er mit dem heutigen Motto „*Innovation, IT und deren Effekte auf die Welt sind meine Passion!*“ in der Welt der IT zu Hause.

RH: Herr Bange - wie sicher sind Ihre Zielgruppen mit dem Thema IT-Security. Treffen Sie eher auf IT- Security-Experten oder auf Neueinsteiger also auf generisch Ratsuchende?

> *SB: Aufgrund unserer sehr heterogenen Zielgruppe ist hier alles dabei. Vom Practitioner, mit unmittelbarem täglichen Kontakt mit ATPs an der Front und umfassendem taktischen Wissen bis zum CISO mit eher abstrakten Wissen und einer Strategie. Oh, und den „bei uns gibt's doch nix zu holen"-CISO mit ausgeprägtem Dunning-Kruger Syndrom[4] - also tendenziell nicht ratsuchend – gibt es auch. Generell kann man sagen, dass die Zielgruppe sehr gemischt ist.*

[2] Die Software sucht kompromittierte Daten der jeweiligen Kunden in Milliarden von Quellen im Open-, Deep- und Darkweb, filtert diese maschinell vor und übergibt die Ergebnisse nach Verifizierung durch einen menschlichen Analysten mit einer sogenannten Zero False Positive Garantie

[3] Der Service beinhaltet das permanente, globale Scanning nach gefälschten Domains, geleakten Credentials sowie die Überwachung der externen Angriffsfläche der Kunden.

[4] https://de.wikipedia.org/wiki/Dunning-Kruger-Effekt

RH: Würden Sie sagen, das auf dem Markt derzeit angebotene IT-Sicherheits-Produktangebot wird den Herausforderungen, die sich durch immer neue Sicherheitslücken und. Angriffstechnologien ergeben, gerecht?

SB: Ich denke nur ein verschwindend kleiner Anteil der aktuell angebotenen Lösungen stellt sich den immer mehr in den Vordergrund tretenden Herausforderungen. Egal, wohin Sie schauen: Neun von Zehn erfolgreichen Attacken gegen ein Unternehmen beruhen auf dem Missbrauch oder im Englischen „Weaponization" der kompromittierten Unternehmensinformationen. Viele Unternehmen haben das noch nicht verstanden und haben noch immer eine Perimeterstrategie im Einsatz, obwohl es den Perimeter entweder nicht mehr gibt oder die Leute dessen Verlauf aufgrund immer komplexer werdender System- und Informationsstrukturen nicht mehr verstehen. Der Permiterschutz ist nach wie vor richtig und wichtig, ist aber nicht mehr ausreichend.

Herr Bange - was fehlt Ihrer Meinung nach am dringlichsten im Markt für IT-Sicherheitsprodukte und - dienstleistungen und wo erkennen Sie in diesen Defiziten die gravierendsten Einfallstore in IT-Infrastrukturen bzw. Fallen für den Faktor Mensch?

SB: Das geht ein wenig in Richtung der vorherigen Frage. Die größte Herausforderung sind meines Erachtens die eben genannten Informationen. Hier fehlt es an Lösungen. Aufgrund Integrationen mit Lieferkette, Audits, Kunden, Mitarbeitern sind von jedem Unternehmen missbrauchsfähige Informationen unterwegs. Sie schicken jedem Mitarbeiter einmal im Monat eine Gehaltsbescheinigung. Die legt der irgendwo, vermutlich mittlerweile auf einem NAS oder in einer Cloud ab. Wenn ich als Theat Actor diese finde, rufe ich einfach im Unternehmen an, lasse mich mit Vor-und Zunamen verbinden, erzähle dem Mitarbeiter dass ich der HR-Dienstleister bin, lese ihm seine Personalnummer vor und motiviere ihn auf Basis des generierten Vertrauens zu verschiedensten Handlungen. Mit personenbezogenen Informationen über den MA kann ich ein Vertrauen schaffen, das auch durch Security Awareness Trainings nicht beeinflusst wird. Der Faktor Mensch ist einfacher zu manipulieren als Maschinen, Informationen helfen dabei und hier gibt es die gravierendsten Defizite in den Strategien der meisten Unternehmen.

RH: Was sind denn die derzeit größten Bedrohungen im IT Sicherheitsbereich?

SB: Informationsmissbrauch der eigenen Unternehmensdaten. Das eben genannte Beispiel des Social engineering, technische daten über sich im Einsatz befindliche Systeme, Audit-Reports, Verträge mit der Lieferkette. Gerade die letztgenannten sind nicht nur ein Risiko aus der IT-Sicherheitsperspektive sondern ganz klassisch kaufmännisch für Beschaffung, Produktion und Absatz. Hier bestehen massives auch finanzielle Risiken, die für die meisten Leute im C-Level eines Unternehmens leider noch immer viel zu abstrakt sind.

RH: Wie hoch schätzen Sie das Sensibilisierungslevel gerade bei IT-ferneren Organisationen und Wirtschaftsunternehmen hinsichtlich Gefahren, Schäden und einer klaren Risikoabschätzung ein?

SB: Hier sind wir beim eben genannten C-Level. Der 64-jährige Seniorchef eines deutschen Mittelständlers, sagen wir - eines hidden Champion [5]im Hochtechnologiebereich - versteht einfach nicht, warum der 15 Jahre alte Server, der irgendwo in der Ecke steht, ein massives Risiko birgt. Der hat doch immer gut funktioniert. Warum sollen wir da was neues kaufen? Ist natürlich ein extremes Beispiel aber der „bei uns gibt's doch nichts zu holen" Gedanke ist leider noch immer sehr weit verbreitet. Die potentiellen Risiken für Unternehmenswert, Umsatz und Reputation sind einfach zu abstrakt als dass diese Transferleistung erbracht werden kann.

RH: Und wie sieht es mit diesem Bewusstsein bei Behörden, Kommunen und anderen öffentlichen Auftragnehmern?

SB: Nehmen Sie mein letztes Statement über Unwissenheit und nehmen Sie das mal 4. Meine Frau ist Lehrerin in NRW. Stellen Sie sich vor, ein Unternehmen hat eine BYOD policy, ohne dass jemand ein Gerät zertifiziert, alle sind völlig ahnungslos, die Infrastruktur fehlt oder ist 20 Jahre alt, es gibt niemanden der hier wirklich verantwortlich ist und alle improvisieren. Ich halte das für exemplarisch in Behörden, Kommunen und öffentlichen Organisationen. Das ist einfach dramatisch. Problematisch ist in diesem Zusammenhang neben der Infrastruktur natürlich auch fehlendes, qualifiziertes Personal. Aber wer kann es den Leuten verdenken? Wenn jemand ein Angebot in der Stadtverwaltung für ein Beamtengehalt von A12 bekommt und in der Industrie ein Äquivalent von A36 verdienen kann, welche Fachkraft fängt denn da bei der Stadtverwaltung an? Hier sind einfach umfassende Reformen erforderlich, auch wenn es teuer wird. Langfristig ist die Reform günstiger als der Effekt des „wir machen mal einfach so weiter und hoffen das Beste".

RH: Könnte die Forschung da helfen? Was wünschen Sie sich von der IT-Sicherheitsforschung?

SB: Unabhängig vom Ergebnis verständlichere Kommunikation, die auch der breiten Masse ermöglicht, die Effekte der Bedrohung für Ihr eigenes Leben zu verstehen. Im Sinne von: „Wenn Du ein schwaches Passwort wählst, ist das so ähnlich als wenn Du zuhause die Haustür offenstehen lässt und zum Einkaufen fährst". Alle IT-Sicherheitsforscher denken, dass ist eine Selbstverständlichkeit. Diese Gedanken sind aber in der breiten Masse der Bevölkerung noch nicht angekommen. Diesen Wissenstransfer sehe ich aktuell als eine der Hauptaufgaben.

RH: Und was würden Sie sich von der Politik wünschen, Herr Bange?

SB: Dass zur Abwechslung einmal kompetente Leute an die richtigen Positionen kommen und Impulse wie z.B. den vorgeschlagenen Maßnahmenkatalog des CCC zumindest in Teilen anfangen umzusetzen.

RH: Herr Bange – abschließend noch drei schnelle Fragen zu Ihrem persönlichen Verhalten in der IT-Security - wie sicher fühlen Sie sich selbst im Umgang mit Ihren individuellen Aufgaben, Prozessen und Technologien – gerade auch vor dem Hintergrund „Arbeiten im Home Office?

[5] Kurze Fußnote zu Hidden Champions

SB: Sicher! Das liegt aber daran, dass man mit den Jahren in der Branche eine gesunde Paranoia entwickelt und sich schützt.

RH: Und wie ausgeprägt ist Ihre Bereitschaft zu Einbußen in der Bequemlichkeit zu Gunsten eines höheren IT-Sicherheitslevels?

SB: Meine persönliche Bereitschaft ist da sehr hoch, ich ziehe mir aber auch Schutzkleidung an, bevor ich mich aufs Motorrad setze. Ich sehe aber viele Leute mit Jeans und T-Shirt auf dem Zweirad, das ist in der virtuellen Welt nicht anders.

RH: Zum Schluss eine schwierige Fachfrage (die in der breiten Diskussion sehr unterschiedlich beantwortet und interpretiert wird) – Was verstehen Sie unter einer Advanced Persistent Threat?

SB: Eine APT würde ich eher als Gruppe denn als Einzelangriffsvektor beschreiben. Eine Threat Actor Gruppe als Advanced Persistent Threat, welche mit TTPs[6] vorgeht. TTPs werden mittlerweile auf unterschiedlichste Weise beschrieben, die auf die eine oder andere Art eigentlich immer auf den alten Lockheed Martin Killchain approach[7] zurückgehen. Die meisten denken in diesem Zusammenhang vermutlich auch an MITRE Att&ck[8]. Dabei geht es um die Angriffsfläche, um Angriffsvektoren und um Informationsmissbrauch.

Herr Bange – haben Sie vielen Dank für Ihre Zeit und für das Interview.

Interviewpartnerin 2: Pauline List (PL),

Frau Pauline List hat Ethnologie und Volkswirtschaft an der Ludwig-Maximilian-Universität München studiert und konzentrierte sich darin auf transnationale Kommunikation. Seit ihrer Übersiedlung in ihre Wahlheimat Israel vor 4 Jahren beschäftigt sie sich mit Themen der Cybersicherheit. Durch entsprechende Engagements bei IT-Security-Unternehmen lernte sie Lösungsansätze für IT-Sicherheitsprobleme zunächst in der Kundenbetreuung und der Projektentwicklung für die DACH Region kennen. Heute ist sie in der Welt der Startups, neuen Technologien und Cyberdeception unterwegs. Frau List arbeitet als Marketingexpertin und Cybersecurity Beraterin bei der Firma „TrapX Security“, einem StartUp, dessen Angriffs-Erkennungslösung auf dem Konzepts von „Honeypots[9]“ aufbaut, diese vereinfacht und für die

[6] Taktiken, Techniken und Prozeduren (tactics, techniques, and procedures) definiert etwa bei NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[8] https://attack.mitre.org/

[9] Sogenannte Honeypots (zu Deutsch Honigtöpfe) werden innerhalb von IP-Netzwerken aufgestellt. Ein Angreifer, der in ein avisiertes Netzwerk eingedrungen ist, sucht häufig nach lukrativen Assets (vertrauliche Firmendaten, Mitarbeiterdaten, Passwort-Dateien, geheime Fertigungsunterlagen usw.). Honeypots „tun so“, als wären sie ein derartiges Asset. Ein Honeypot könnte sich zum Beispiel als nachgemachter „File-Share“ oder als Drucker oder als GIT repository ausgeben. Der Angreifer kann nur schwer unterscheiden, was „echte“ Informationen im angegriffenen Netzwerk sind und was Honeypots. Letztere besitzen einen Alarmierungsmechanismus, der die Admins benachrichtigt, wenn auf dem Honeypot Zugriffe registriert werden. Der Netzwerkbetreiben weiß dann, dass ein Angreifer sich im Netzwerk bewegt und kann Gegenmaßnahmen einleiten.

Erkennung von Angreifern im Unternehmensnetzwerk und zur Verhinderung des Ausspähens sensibler Daten für seine Kunden bereitstellt.

RH: Frau List - wie sicher sind Ihre Zielgruppen mit dem Thema IT-Security? Treffen Sie eher auf IT- Security-Experten oder auf Neueinsteiger also auf grundsätzlich Ratsuchende?

> *PL: Unsere Produkte richten sich an eine tendenziell erfahrene Zielgruppe. Unser Thema Honeypots ist bei IT-Sicherheitsexperten und SOC-Betreibern[10] bekannt. Für IT-unerfahrene ist der Ansatz „Sicherheit aus der Vorgehensweise der Angreifer abzuleiten" zunächst ungewohnt, allerdings etwa über MSSP (Managed Security Service Provider) auch leicht zugänglich. Entsprechend sprechen wir häufig von IT-Sicherheitsexperten zu IT-Sicherheitsexperten. Ich persönlich freue mich aber besonders über Interesse und Anfragen von Neueinsteigern, die oft eine frische Perspektive mitbringen.*

RH: Also ein sehr komplexes Produkt - würden Sie sagen, das auf dem Markt generell verfügbare IT-Sicherheits-Produktangebot wird den Herausforderungen gerecht, die sich durch immer neue Sicherheitslücken und Angriffstechnologien ergeben?

> *PL: Eher eine komplexe Idee in einem einfachen Produkt. Besonders interessant finde ich, dass der Honeypot-Ansatz Unternehmen zu einem Perspektivwechsel anregt. Auf dem Markt gibt es eine kaum zu Überblickende Vielzahl verschiedener Produkte und Lösungen für eine Vielzahl kundenspezifischer Problemstellungen und Gefahrenvektoren. Was allerdings bedenklich stimmt ist, dass gerade in der DACH Region die Gesetzeslagen oft den Einsatz bestimmter Technologien nicht erlauben oder zumindest stark beschränken. Denken Sie da nur an Werkzeuge zur „Behavioral Analytics". So entstehen gewissermaßen Lücken in der Phalanx der Abwehrtechnologien.*

RH: Spannend, habe ich so noch nie betrachtet - was fehlt Ihrer Meinung nach am dringlichsten im Markt für IT-Sicherheitsprodukte und -dienstleistungen und wo erkennen Sie in diesen Defiziten die gravierendsten Einfallstore in IT-Infrastrukturen bzw. Fallen für den Faktor Mensch?

> *PL: Am meisten fehlen Cybersecurity-Spezialisten mit einem breiten IT und IT-Security-Überblick. So in der Art von „Cybersecurity-Architects". Und es fehlt in Europa ein Stück weit an IT-Experten, die sich mit dem Themenfeld „Risikoevaluationsmodelle" a la FAIR[11] beschäftigen. In den Vereinigten Staaten etwa wenden zahlreiche CIOs bereits heute konsequent das aus der Praxis von CISOs entwickelte „Factor Analysis of Information Risk" (FAIR) Modell zur Auslegung und Überprüfung ihrer IT-Sicherheitsarchitektur an. Dem hinken IT-Verantwortliche in Deutschland bisweilen noch deutlich hinterher.*

RH: Was sind Ihrer Meinung nach die derzeit größten Bedrohungen im IT-Sicherheitsbereich?

---

[10] SOC: Security Operation Center – ein organisationsinterner oder -externer Dienst, der kontinuierlich die IT-Sicherheit in der IT der Organisation überwacht und bei erkannten Angriffen Alarm schlägt und Abwehr-/ Erkennungs-/ Gegenmaßnahmen einleitet.

[11] Etwa hier: https://securityintelligence.com/posts/using-fair-and-nist-csf-security-risk-management/

PL: In meiner Beobachtung hat der „Human Factor“ als Angriffsziel erst durch eine vorangegangene Problematik so große Bedrohung erlangt: Der Mensch als Verursacher eines kaum zu durchblickenden Datenchaos in seinen Arbeitsabläufen und deren Digitalisierung ist das primäre Problem und mitverursacht unbedachtes Fehlverhalten. Mitarbeitende im Unternehmen stehen unter Zeitdruck und agieren mit großen Datenmengen. Da ist es nur naheliegend, dass wir alle nicht für jede Datei, für jedes Dokument die jeweils besten Schutz- und Storage-Verfahren nutzen. Und das können Angreifer gezielt ausnutzen. Außerdem gibt es oft zu viele Kommunikations- und Datenhaltungssysteme innerhalb einer Organisation. Das kann kaum noch jemand überblicken.

RH: Wie hoch schätzen Sie das Sensibilisierungslevel gerade bei IT-ferneren Organisationen und Wirtschaftsunternehmen hinsichtlich Gefahren, Schäden und einer klaren Risikoabschätzung ein?

PL: Wie vorhin schon erwähnt, kommen wir mit diesen Zielgruppen aufgrund des hohen IT-Sicherheitsgrundwissens, das zur Benutzung unserer Produkte erforderlich ist, eher selten in Berührung. Es fällt mir schwer, diese Frage valide zu beantworten.

RH: Frau List, dann erspare ich Ihnen die folgende Frage zum Sensibilisierungslevel von Behörden und springe gleich zur Anschlussfrage - was würden Sie sich von der IT-Sicherheitsforschung wünschen?

PL: Da fallen mir sofort zwei wichtige Aspekte ein. Zum einen sollte die Forschung in ihren Wissenstransferbemühungen eine einfache Sprache suchen, um von breiten Zielgruppen verstanden zu werden, denn das Thema Informationssicherheit betrifft uns alle – und weiterhin wäre es meiner Meinung nach eine ganz dringliche Aufgabe gerade für die Cybersecurity-Forschung, sprachliche Brücken und Abgleiche zu schaffen zwischen der deutschen und der englischen IT-Sicherheitsfachsprache. Allein durch die Anwendung von zweierlei Sprachräumen entstehen so viele Unsicherheiten und Unschärfen. Denken Sie nur an die beiden grundverschiedenen Bedeutungen von Safety und Security im Englischen, die im Deutschen in beiden Fällen durch Sicherheit übersetzt werden.

RH: Und was würden Sie sich von der Politik wünschen?

PL: Es wäre toll in Deutschland mal eine Regierung zu haben, die IT-Sicherheit, und Digitalisierung wirklich vorlebt. Der CCC [12]hat ja recht klare Erwartungen an die neue Koalition gestellt. Ich bin sehr gespannt, ob diese das umsetzen kann und wird.

RH: Frau List – abschließend auch an Sie noch drei schnelle Fragen zu Ihrem persönlichen Bewusstsein gegenüber der IT-Sicherheit - wie sicher fühlen Sie sich selbst im Umgang mit Ihren Aufgaben und Prozessen – gerade vor dem Hintergrund „des Home Office?

PL: Mein Lebens- und Arbeitsmittelpunkt ist seit 4 Jahren Tel Aviv. Meine israelischen Kolleginnen und Kollegen sind durchwegs durch die politische und gesellschaftliche Situation mit einem Sinn für Sicherheit gesegnet. Und das übertragen wir in alle Arbeitsabläufe und auch in unsere Produkte, Entwicklungen und Beratungsgespräche.

[12] https://www.ccc.de/de/updates/2021/ccc-formulierungshilfe-regierungsprogramm

Daher fühle ich mich insgesamt in meinen Prozessen und in meiner Arbeitsumgebung – auch im Home Office ziemlich safe.

RH: Und wie ausgeprägt ist Ihre Bereitschaft zu Einbußen in der Bequemlichkeit zu Gunsten eines höheren IT-Sicherheitslevels?

PL: Naja – wir machen konsequent Zweifaktorauthentifizierung bei der Anmeldung am Endpoint und an zentralen Systemen. Händische Verschlüsselungsverfahren musste ich noch nie anwenden, womöglich würde meine Geduld hier an ihre Grenzen stoßen.

RH: Zum Schluss auch an Sie, Frau List meine schwierige Lieblingsfrage – wie würden Sie persönlich den Gefahrenvektor Advanced Persistent Threat beschreiben?

PL: Das ist ein viel diskutiertes Thema bei uns im Unternehmen, da unsere Technologie eben keine „Außengrenzen" schütz, sondern Angreifer aufspürt, die erste Schwachstellen oder Unbedachtheiten ausgenutzt haben und nun das Interne-Netzwerk erkunden. APTs sind gewissermaßen die Königsdisziplin aller Cyberthreats. Da sitzen wirkliche Menschen an den Angriffs-Computern und kombinieren automatisierte und manuelle Verfahren, um menschliche und organisatorische Schwachstellen auszunutzen. Es gibt einen bekannten Spruch in der IT-Sicherheitswelt, der hier gut passt: „Jedes System ist „hackbar", es ist nur eine Frage der eingesetzten Zeit und Ressourcen.

Frau List – ganz herzlichen Dank für Ihre Zeit und für das Interview.

Interviewpartner 3: Ramon Mörl (RM),

Ramon Mörl ist seit 2002 Geschäftsführer der itWatch GmbH und hat 30 Jahre Erfahrung als Berater in der IT-Sicherheit. Zu seinem Portfolio gehören leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA. Als unabhängiger Evaluator und Berater der Europäischen Union war Herr Mörl vor allem im Bereich der ECMA und an ISO-Standards für die IT-Sicherheit tätig. Der Fokus der Firma itWatch GmbH liegt auf dem Schutz vor Datendiebstahl (Data Loss Prevention - DLP), auf technischen Vertrauensketten von der Tatstatur bis zu den Daten, sowie deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Security), Datenschleuse mit Datenwäsche sowie Mobile Security und Verschlüsselung. Erste Produkte wurden bereits 1997 entwickelt.

RH: Herr Mörl - wie sicher sind Ihre Zielgruppen mit dem Thema IT Security. Treffen Sie eher auf IT-Security-Experten oder auf Neueinsteiger also auf generisch Ratsuchende?

RM: Wir können mehrere Zielgruppen unterscheiden. Zum einen gibt es die „alten Hasen", die wir hauptsächlich bei Familienunternehmen mit wenig Fluktuation und bei Kunden antreffen, in deren Umfeld IT-Sicherheit schon immer wichtig war – z.B. Polizei, Militär und Nachrichtendiensten. Dann gibt es klassische Mainstreamkunden, die den Weg nur selten zu „best oft the breed"-Lösungen schaffen. Bei diesen wechseln die IT-Mannschaft und die IT-Security-Verantwortung regelmäßig, so dass es kein nachhaltig

bewirtschaftetes Thema ist. Die dritte Gruppe sind die Newcomer. Meist sind das dann Unternehmen, bei denen die IT-Sicherheit durch einen Vorfall direkt im Haus oder in deren Nähe spontan an Wichtigkeit gewinnt. Die Personen in diesen Unternehmen sind meist Neueinsteiger in das Thema oder waren bisher mit anderen Themen betraut, denn „das mit der IT-Sicherheit kann ja auch nicht so schwer sein".

Bei den beiden letzten Zielgruppen zeigt sich die Wichtigkeit Ihrer Frage. Im gesamten Entscheidungsprozess fehlt die Entscheidungskompetenz darüber, was „wirklich immer schützt" und „was nur manchmal oder meistens schützt". Die Frage nach der Mechanismusstärke des Schutzes und der darüber erzielbaren Resilienz gegenüber Angriffen ist aber nach meiner Erfahrung das Entscheidende bei der Beschaffung und Implementierung von Schutzprodukten. Lassen Sie mich ein Beispiel erzählen, dass es nicht immer nur an der Kompetenz der technischen Abteilung liegt: Wir hatten bei einem DAX-Unternehmen eine 6-monatige Testphase von mehreren Produkten – das itWatch Produkt war eines davon. Die Testmannschaft war sehr gut informiert und hat sehr komplizierte Tests durchgeführt und kam nach sechs Monaten zu dem Schluss, das itWatch Produkt als „best oft the breed" zu kaufen. Der Einkauf veränderte das Szenario und organisierte eine Internetversteigerung – unabhängig von der Mechanismusstärke des Produktes, also nur nach dem Preis. Das billigste Produkt gewann. In der Konsequenz hat man die Anforderungen an den Einsatz nachträglich nach unten gesetzt, weil das bestellte Produkt eben nicht geeignet war für den Roll-Out.

RH: Würden Sie sagen, dass auf dem Markt derzeit angebotene IT-Sicherheits-Produktangebot wird den Herausforderungen, die sich durch immer neue Sicherheitslücken und Angriffstechnologien ergeben, gerecht?

RM: Ein klares Nein. Es gibt eine ganze Menge von Produkten, die den Anforderungen durch immer neue Angriffe wirklich gerecht werden – aber der Nutzer kann diese nicht von „Fake Security"-Produkten unterscheiden. Produkte deren Hersteller ihr Kapital zu großen Teilen für Marketing und zu geringem Anteil für die technisch notwendige Forschung ausgeben, bleiben häufig in dem Schutzversprechen hinter der Erwartung des Marktes zurück. Aber einmal gekauft wird das Thema eben frühestens nach drei Jahren wieder „angefasst". Leider ist dadurch auch der Markt für sinnvolle Lösungen oft für längere Zeit blockiert.
Ein Beispiel dazu kann in dem Thema Sandboxing und Virtualisierung beobachtet werden. Hier haben sich viele sinnvolle und auch weniger sinnvolle Lösungen einen Markt erarbeitet. Die wenigsten Kunden identifizieren aber, wenn sie z.B. auf Applikationsvirtualisierung setzen, dass der Content, der in den Applikationen bearbeitet wird, dann doch z.B. für die Druckaufbereitung in die produktiven Netze kommt, weil bei den gängigen Lösungen nicht alle Hintergrundprozesse virtualisiert werden. Aus diesen Gründen hatte das BSI, als es das ReCoBS-Profil für den sicheren Einsatz von Browsern[13] veröffentlichte, auch bestimmte Verfahren ausgenommen.

Herr Mörl - was fehlt Ihrer Meinung nach am dringlichsten im Markt für IT-Sicherheitsprodukte und - dienstleistungen und wo erkennen Sie in diesen Defiziten die gravierendsten Einfallstore in IT-Infrastrukturen bzw. Fallen für den Faktor Mensch?

13

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf?__blob=publicationFile

RM: Herr Schönbohm, der Präsident des BSI, und viele andere für die IT-Sicherheit wichtige Personen und Organisationen, betonen immer wieder, dass wir nur dann gegen die Angriffe geeignet gerüstet sind, wenn wir zusammenarbeiten. Dieser Erkenntnis stimme ich zu 100% zu – leider wird sie nicht gelebt und noch schlimmer die tatsächlichen Maßnahmen sind oft kontraproduktiv. In dem IT-Sicherheitsgesetz 2.0 und den weiteren Regulierungen dazu wird z.B. sehr stark auf Diversität gesetzt, um nach erstem Verständnis unabhängig zu sein und immer einen Dienstleister zu haben, der in die Leistung geht. Dabei wird aber verkannt, dass die Ziele Verfügbarkeit auf der einen Seite und Integrität und Vertraulichkeit auf der anderen Seite, häufig im Gegensatz stehen. Ein einfaches Beispiel: Man möchte alle Dateien auf allen Servern verschlüsseln, um auch in anderen Regionen speichern zu können. Um nicht abhängig von einem Produkt und einem Dienstleister zu sein, kauft man zwei Produkte von zwei Lieferanten und fordert Kompatibilität, so dass mit jedem der beiden Produkte alle Dateien entschlüsselt werden können. Hat nun auch nur eines der beiden Produkte eine Hintertüre oder eine Schwachstelle, so sind alle Daten – auch die von dem zweiten verschlüsselten – offengelegt. Der Verlust der Vertraulichkeit wurde also dem Ziel der Verfügbarkeit „geopfert", obwohl das Produkt eigentlich Vertraulichkeit sichern sollte.
Was heisst das jetzt für den Faktor Mensch? Bruce Schneier, ein Urgestein der Kryptographie, sagte in einer emotionalen Rede auf der Münchner Cyber Security Konferenz (mcsc), die immer einen Tag vor der Münchner Sicherheitskonferenz (msc) stattfindet, dass wir aufhören müssen den Anwender vor bestimmten Aktionen in der IT zu warnen (USB Sticks, Mail Attachments und Browser Downloads) und endlich anfangen müssen, sichere IT- Systeme zur Verfügung zu stellen, so dass sich der Anwender ohne schlechtes Gewissen auf seine Tätigkeit konzentrieren kann. Das ist eine kooperative Anstrengung. Wenn wir uns den Straßenverkehr ansehen, dann stellen wir fest, dass auch dort etwas passieren kann, aber viele Regeln über die letzten 100 Jahre eingeführt wurden, die die Unfallhäufigkeit aber auch den entstehenden Schaden reduzieren. Dazu tragen viele Themen bei. In der IT haben wir kaum die Möglichkeit für Haftung und es gilt ein „schütz Dich selbst sonst schützt Dich niemand". Die Steuergelder werden nicht zum Schutz der Bürger und ansässigen Unternehmen im Cyberraum ausgegeben. Auch an dieser Stelle halte ich Kooperation für zwingend notwendig.

RH: Was sind denn die derzeit größten Bedrohungen im IT-Sicherheitsbereich?

RM: Auf der ITSA habe ich gerade einen Vortrag mit dem Titel „Jeder Cyber-Angriff braucht Soft- oder Hardware - z.B. Ransomware einfach rauswaschen - wie geht das?" gehalten*. Ich denke die größte Bedrohung ist, dass viele neue Technologien, die neue Fähigkeiten, mehr Spaß, einfacheren Betrieb, weniger Ärger oder Ähnliches versprechen, eben auch neue Tore öffnen. Zum Beispiel Codeelemente – also kleinste Stückchen Software – die in IT-Werkzeuge integriert werden und bei denen sich niemand Gedanken macht, wie wir darin gut von böse unterscheiden können. Am Ende vom Tag muss man aber, wenn man seine IT-Umgebung sicher managen will, jedes Stückchen Software und die in der Hardware verbauten Elemente wie Controller kennen, denn man kann nur managen was man kennt.*

RH: Wie hoch schätzen Sie das Sensibilisierungslevel gerade bei IT-ferneren Organisationen und Wirtschaftsunternehmen hinsichtlich Gefahren, Schäden und einer klaren Risikoabschätzung ein?

RM: In Ihrer ersten Frage hatte ich bereits drei Kategorien aufgemacht. Familienunternehmen mit guten Margen sind sich ihrer Stellung bewusst und versuchen ihren Besitz auch die IP und ihre intellektuellen Assets geeignet zu schützen. Bei Managern, die einen typischen Wechsel nach drei Jahren haben, ist das Erfüllen der eigenen Ziele für ihre Boni höherwertig, so dass hier oft nicht nachhaltig gearbeitet wird. Insofern hat es nach meiner Wahrnehmung weniger mit der Branche oder der Distanz zur IT zu tun.
Etwas ist aber auffällig: Durch die Digitalisierung von Standardprodukten, wie Staubsaugern, Lampen, Rauchmeldenr etc. kommt das IT-Risikomanagement des Herstellers dieser Produkte bis ins Schlafzimmer der Kunden. Was meine ich damit: Stellen Sie sich vor, Sie wissen welches Modell eines Staubsaugerroboters ihr Nachbar einsetzt. Sie gehen in den Laden, kaufen ein baugleiches, öffnen es und setzen eine Kamera, ein Mikro und ein WLAN ein. Sie schicken das an ihren Nachbarn mit einem schönen Entschuldigungsschreiben des Herstellers, dass in dem alten Modell leider der Akku überhitzen kann und schwupp-di-wupp haben Sie fahrbare Augen und Ohren beim Nachbarn in allen Zimmern.
Nach meiner Wahrnehmung müsste der Hersteller sich um seine Kunden sorgen und das Risikomanagement für sie übernehmen und gegen diesen Angriff schützen. Dann wäre sein Produkt aber teurer und später auf dem Markt. Wie können wir also bei der Digitalisierung der Gesellschaft rote Linien ziehen und das Filmen in fremden Schlafzimmern nicht dem Risikomanagement eines Staubsaugerherstellers überlassen?

RH: Starkes Beispiel Herr Mörl! Wir sind gespannt, wie viele unserer Leserinnen und Leser nach diesem Statement ihre Saugroboter mal ganz genau unter die Lupe nehmen werden. Sagen Sie - wie sieht es mit diesem Bewusstsein bei Behörden, Kommunen und überhaupt bei öffentlichen Auftragnehmern aus?

RM:
Wahrscheinlich treffen wir hier die größte Diskrepanz zwischen Wunsch und Wirklichkeit an. KMU in jeder Region nehmen sich ihre Kommunen und kommunalen Unternehmen oft als Vorbild, denn die wissen ja genau was Gesetz ist und bekommen ganz sicher gesagt wie man die IT schützt. Leider ist das aber nicht so.
Ergebnisse von Marktuntersuchungen einer Behörde, die mit Steuergeldern finanziert wurden, stehen anderen steuerkonsumierenden Organisationen nicht zur Verfügung. Insofern bekommt die Kommune leider keinen Hinweis von dem BND, dem BKA oder ihrer lokalen Polizei, welche IT-Sicherheitsprodukte gut schützen würden, sondern muss sich auf die Expertise der eigenen Mitarbeiter oder die Gespräche in verschiedenen Gremien verlassen. Alle Gremien sind aber zur Neutralität verpflichtet, so wird der Städte- und Gemeindetag dieses Defizit auch nicht beheben.
Die IT-Sicherheit ist in diesem Punkt deshalb anders, weil es keine definierte Metrik und keine sichtbare Funktionalität gibt. Bei anderen IT-Produkten erkennt man relativ leicht, ob sie ihre Funktion, für die man sie einkaufen will, auch leisten. Bei IT-Sicherheit eben nicht. Deshalb wäre es besonders wichtig, die Mechanismusstärke von Produkten in den Gremien darzustellen.

RH: Könnte die Forschung da helfen? Was wünschen Sie sich von der IT-Sicherheitsforschung?

RM: Drei Dinge wären mir besonders wichtig: Erstens sollte dringend an Verfahren zum Messen der Robustheit gearbeitet werden – also wie gut schützt ein Produkt. Zweitens müssen die Forschungsergebnisse sinnhaft in die Nutzung überführt werden. Es hilft uns nichts, wenn wir Forschungsweltmeister sind, aber keine Wertschöpfung aus den Forschungsergebnissen stattfindet. Drittens: Wenn wir feststellen, dass etwas, was wir uns gewünscht haben, nicht so funktioniert wie wir dachten, dann müssen wir interdisziplinär anfangen zu forschen, was noch fehlt.
Dazu ein paar Beispiele: Wenn wir feststellen, dass wir durch Weitergabe der Marktsichtungsergebnisse zwischen steuerkonsumierenden Organisationen zum einen Geld sparen können und zum anderen höhere Sicherheit erreichen, dann darf der Einwurf „das Vergaberecht steht dem Austausch entgegen" nicht verhindern, sondern muss zum Forschen anregen, wie wir es hinbekommen. Wenn Frau Merkel ihr sicheres Handy nicht nutzt, weil die Sicherheitsfunktionen ihre Ergonomie beeinträchtigen, müssen wir forschen, wie wir das Handy „Kanzlerin-tauglich" machen.

RH: Da sind wir fast schon bei meiner nächsten Frage - die Politik – was würde Sie sich von dieser wünschen?

RM: In erster Linie mehr Kooperation. Dazu zählt, dass der Staat ein Schutzversprechen gegenüber seinen Bürgern und den ansässigen Organisationen abgibt, dieses aber im Cyber-Raum nicht erfüllt. Wieder stehen natürlich viele Gründe gegen einen Schutz aller Bürger im Cyber-Raum, aber wenn wir nicht anfangen dazu zu forschen und nachzudenken, wie wir einen Basisschutz und eine starke Reduzierung der Cyber-Kriminalität als Gesellschaft hinbekommen, dann wird die Digitalisierung auf zweifelhaftem Boden gebaut.

RH: Herr Mörl – abschließend noch üblichen drei Abschlussfragen zu Ihrem persönlichen Verhalten in der IT Security - wie sicher fühlen Sie sich selbst im Umgang mit Ihren individuellen Aufgaben, Prozessen und Technologien – gerade auch vor dem Hintergrund „Arbeiten im Home Office?

RM: Bestens gerüstet. Ich mache seit 30 Jahren IT-Sicherheit als Kernthema, da ist es tatsächlich egal wo ich arbeite. das adäquate Schutzniveau kann ich immer gut einhalten – allerdings verzichte ich auf viele „Innovationen", die mir verdächtig erscheinen.

RH: Und wie ausgeprägt ist Ihre Bereitschaft zu Einbußen in der Bequemlichkeit zu Gunsten eines höheren IT-Sicherheitslevels?

RM: Natürlich bin ich bereit zu einem anderen Verständnis. Ich benutze drei Handys und mehrere Rechner. Ich würde nie eine Videokonferenz nativ auf meinem Firmenrechner durchführen oder meine Authentisierung zu Firmenkonten (auch E-mail) auf einem fremden Rechner vornehmen.

RH: Zum Schluss eine schwierige Fachfrage – Was verstehen Sie unter einer Advanced Persistent Threat?

RM: Es handelt sich um eine hochwertige, dauerhaft präsente Bedrohung, die unterschiedliche Angriffsvektoren nutzt, um immer weiter in ein System oder eine Organisation einzudringen. Hochwertig deshalb, weil nicht die sofortige Monetarisierung gesucht wird – wie beispielsweise bei Ransomware – und deshalb sehr viel Wert auf Verschleierung des Angriffs gelegt wird. Dauerhaft präsent deshalb, weil tatsächlich echte Menschen mit Know-how auf der anderen Seite sitzen und sich die Abfolge der Angriffe so ausdenken, wie es gerade passend erscheint, so dass der Angriff insgesamt erfolgreich wird. Es entsteht also eine Folge von aufeinander aufbauenden Angriffen, die insgesamt ein längerfristiges Ziel verfolgen und während dieses Zeitraums nicht erkannt werden dürfen.

Herr Mörl – haben Sie vielen Dank für Ihre Zeit und für das Interview.