35 Jahren Cyber-Security als Wirtschaftsfaktor:
Erfolge mit Innovation und Startup in der Schweiz.
Heiner Kromer, CEO SECUDE international AG, Speech 14.2.2018

Herzlichen Glückwunsch zur Gründung des IT Security Departments. Ich freue mich auf eine gute und langfristige Zusammenarbeit.
Kurz zu meiner Person: Mein Name ist Heiner Kromer und ich bin Chairman & CEO von SECUDE AG.
Meine Ausbildung schloss ich auf der Uni Zürich mit dem Doktor der Betriebswirtschaft ab. Anschliessend zog es mich in die USA. Ich wollte Unternehmer werden und war der Meinung, dass ich in den USA bessere Chancen habe etwas ohne eigenes Geld auf die Beine zu stellen. Meine erste Firma gründete ich 1968 in New Jersey. In den folgenden 35 Jahren gründete ich in den USA 17 Unternehmen bzw. Tochtergesellschaften. 2002 übernahm ich eine wacklige SECUDE. Ich war erfolgreich und verkaufte SECUDE 2011 an SAP.

Nach dem Exit startete ich die zweite Auflage von SECUDE (SAP überlies mir den SECUDE Namen) mit einer neuen IT Security Idee: Halocore. Diese Technologie basiert darauf, SAP Log Daten zu erfassen und zu analysieren, die aus SAP Exit Points heruntergeladen werden können und diese Daten mit Microsoft RMS zu schützen.

Meine Startup Erfahrung umfasst überwiegend den High-Tech Markt. Zum Beispiel Biotech, Labormessgeräte, Specialty Chemicals, Thermostate, medizinische Geräte, Mess- und Regeltechnik und schliesslich IT Security Software.

Mit der IT-Fachhochschule arbeitet SECUDE schon sehr lange zusammen. Während dieser Zeit habe ich sehr intensiv mit Professor Hämmerli zusammengearbeitet. Er wurde von mir in unser Advisory Board berufen. Auch bei der Neugründung von SECUDE in 2011 war Prof. Hämmerli an der Entwicklung Strategie beteiligt. Prof. Hämmerli hat mir auch geholfen mein Kader aufzubauen. Meine R&D Führungskräfte kamen über ihn zur SECUDE.
Wie Sie sehen eine tiefe und erfolgreiche Zusammenarbeit zwischen Ausbildung und Praxis.
Inzwischen haben wir 3 HALOCORE Patente angemeldet und ein weiteres ist «in the works». Unser Produkt läuft stabil in Production and wir haben erste

Referenzkunden gewonnen mit z.B. Mars, Microsoft und BIT in der Schweiz. Derzeit laufen über 15 Pilots/POC's bei grossen Unternehmen. Bisher sind über 20 Millionen CHF in die Halocore Entwicklung geflossen. Wie sie sehen ist das Investitionsrisiko sehr hoch. Wenn es aber dann funktioniert, ist der Return On Investment aussergewöhnlich.

Die Zusammenarbeit mit der HSLU Informatik Luzern beinhaltet auch konkrete Entwicklungsprojekte. Beispiel: Mit Finanzierungshilfe von Bern, arbeiten wir derzeit mit einem Team der HSLU Informatik an einem Projekt, welches unser Halocore Produkt voll automatisieren soll. Halocore beinhaltet classification von SAP log files. Die Daten müssen heute semi-automatisch bzw. manuell über Templates klassifizert werden. Das gemeinsame Projekt hat zur Aufgabe diese Klassifizierung mit einer «learning engine» voll Automatisch zu lösen.

Ein grossser Integrator mit ca. 480,000 Consultants sagte mir kürzlich: Wir haben eine kritische Lücke von Securityexperten, denn wir können 20,000 offene Security Stellen nicht besetzen. Er schätzt das bis 2020, 200.000 Stellen bei ihrem Unternehmen nicht besetzen können. Weltweit werden von allen Integratoren ca. 1 Million IT security Stellen nicht besetzt werden können. Das hat Konsequenzen auf die Sicherheitslage. Natürlich auch auf die Security Ausbildung. Deswegen müssten sich viel mehr IT Entwickler auf Security spezialisieren.

Der rasante Anstieg der Security Stellen ist angetrieben vom Vormarsch der Cloud, dem Internet der Dinge, sowie der allgemeinen Digitalisierung der Betriebsabläufe. Die rapide Entwicklung von Dronen und Künstlicher Intelligenz ist ein "Game Changer" der eine ernsthafte Bedrohung der Nationalen Sicherheit bedeutet, wenn wir es nicht schleunigst in den Griff bekommen. Das Potential für gezielte Cyber Angriffe durch Staaten die Böses wollen sowie Kriminellen und Terroristen über gefährliche BOT nets, sind äusserst explosive und beängstigend. Gegen dieses Bedrohungspotential müssen wir die offenen IT Security Stellen sehen.
Einer der grössten IT Firmen der Welt ist mir bekannt das dort im letzten Jahr 20,000 IT Stellen nicht besetzen werden konnten. Von einem grossen Integrator weiss ich das sie händeringend SAP Sicherheitsexperten suchen. Man hat es kürzlich aufgegeben nach Experten im Markt zu suchen und versucht nun Quereinsteiger zu schulen. Das sind Fakten, die unserem heutigem Anlass wirklich Bedeutung geben.

Entsprechend hat auch SECUDE in den 16 Jahren in unserem Luzerner HQ permanent Resource Probleme gehabt. Ich war gezwungen QC und Entwicklung ins Ausland zu verlagern. SECUDE kann nur Top-Leute gebrauchen die flexibel, extrem kreativ und voll anpassungsfähig sind. Sie müssen auch mit anderen Kulturen arbeiten können und da liegt oft das Problem. Warum ist das so?
Die meisten Absolventen wollen zu den grossen Schweizer Unternehmen. Grund: Man glaubt es gibt dort Job Security. Das ist aber inzwischen nur ein Mythos mit dem die grossen Unternehmen rekrutieren. Die Realität sieht heute anders aus. Auch diese Unternehmen lassen Leute gehen. Der CIO hat nur eine zwei Jährige Überlebenschance in den USA. Es ist brutal da draussen.
Wer will schon zu einem Start-Up Unternehmen, wenn man nie weiss, ob die Firma überlebt. Es fehlt an Risikobereitschaft. Die wenigsten sehen, das sie in einem Start-up eine viel bessere Sicht auf ein viel breiteres Wissen bekommen. In einem grossen Betrieb sieht man normalerweise nur ein sehr kleines Know-how Fenster. Und das während vieler Jahre! Dagegen kann ein Startup äusserst spannende Aufgaben bringen, die man kaum in einem Grossbetrieb bekommt.

Übrigens: Es ist ein offenes Geheimnis das SAP das gesamte IT SECURITY Development Team von Deutschland nach Bulgarien verlagerte. Letzte Woche teilte uns Coca-Cola mit, dass das gesamte IT Security Team entlassen wurde und die IT Security Function nach Bulgarien verlagert wurde. Grund: Schwierigkeiten Leute zu finden. Man glaubt Bulgarien gibt mehr Fachleute her und dazu zu niedrigeren Kosten.
Daraus sehe ich Konsequenzen für uns in der Schweiz:

- Man muss mehr Top-Leute ausbilden, weil wir mit der Masse an Uni Abgängern International nicht konkurrieren können. Stellen Sie sich vor: Indien produziert jedes Jahr 1,5 Millionen IT Hochschulabgänger. Davon 20,000 IT Security.
  China sogar etwas mehr mit 2 Millionen. Für IT Security habe ich keine Zahlen. Addieren sie USA und Russland Ukraine, Polen, Rumänien Bulgarien, Philippinen, Uruguay und Argentinien, sind die Schweizer Zahlen weit hinter dem Komma. Ich war in den letzten Jahren sehr oft bei Microsoft in Seattle. 90% der Experten die ich traff waren Inder. In der sehr grossen SAP Abteilung habe ich nur eine Amerikanerin angetroffen. Auch der CEO von MS ist Inder. Der Chef für RMS/AIP ist ebenfalls Inder. Überwiegend sind die Inder auf Zeit angestellt und dazu meist Leiharbeiter

von Accenture. Wenn Trump also die Visas wirklich von 150.000 auf 50.000 runterschraubt, hat die IT Branche echte Resourcen Probleme. Gehen sie nicht davon aus, dass das Niveau in Indien nicht so gut ist wie unser Niveau hier. Ohne Zweifel sehe ich mehr und mehr Inder in Führungspositionen. Die Konkurrenz verlangt von uns eine grosse Steigerung des Wissens.

- Wir brauchen mehr angewandte Ausbildung, denn ein Unternehmen wie z.B. Secude, kann niemand mit einen langen Anlauf gebrauchen um produktiv zu sein. Sie müssen sofort Resultate bringen. D.h. wir brauchen mehr gemeinsame Projekte, die zu praktischen Anwendungen führen.
- Diese Ausbildung muss so gut sein, dass die Absolventen wie Fett auf der Suppe hochschwimmen und Führungskräfte werden und nicht als Coder im Mittelmass versinken.
- Der Digitalisierungsprozess ist im vollen Gange. Von CAD zur Produktion von Robotern, zum Internet der Dinge und Cloud Anwendung, an Security geht kein Weg dran vorbei. Leider haben viele Unternehmen noch nicht den vollen Umfang der Gefahren und Risiken erkannt. Man sagt: Bis jetzt ist nichts passiert also wieso muss etwas morgen passieren! Garantiert zu viel Risiko wird hier eingegangen.
- Aus diesem Grund hinken die Verteidiger den Angreifern hinterher, wobei diese jeden Tag aggressiver, besser und gefährlicher werden. Im Krieg der Angreifer und Verteidiger verlieren die Verteidiger derzeit.
  Grund: Es fehlt nicht nur an Experten und Geld, sondern auch am Willlen das SECURITY Thema hart und nachhaltig anzugehen. Es fehlt an politischem Willen, obwohl ich den Security Stand bei uns gegenüber vielen anderen entwickelten Länder, als sehr hoch ansehe.

Integratoren leben sehr gut vom Consulting. Halocore wird – wenn es voll automatisch läuft, Consultants freisetzen. Das haben Integratoren nicht gerne. Allerdings müssen diese Unternehmen jetzt umdenken. Sie bekommen keine Leute. Die einzige Chance ihr Billing hoch zu halten, ist der Einsatz von voll automatischen Produkten. Eine goldene Chance für SECUDE. Das ist auch der Grund warum unser Entwicklungsprojekt mit der Universität Luzern vorangetrieben wird. Der Einsatz von Vollautomation ist notwendig um die Industrie und Business konkurrenzfähig zu halten. Wir müssen Künstliche Intelligenz Projekt einsetzen und das ist auch die Basis für unser HALOCORE Projekt mit der HSLU Informatik.

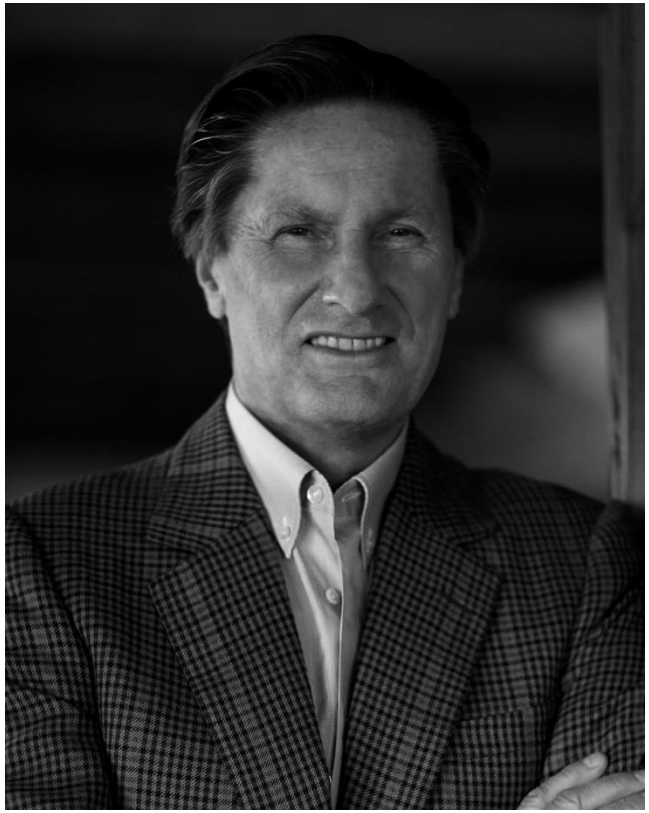
Der Digitalisierungsprozesses ist nicht mehr umkehrbar. Wer es nicht macht, wird unweigerlich unter die Räder kommen.
Ein paar Bemerkungen zur Cloud. Rechenzentrum ist nichts Neues. Eigentlich ein alter Hut. Allerdings, heute bieten die Gorillas Komplettlösungen an, verbunden mit sehr schnellen Verbindungen und vergleichsweise niedrigen Kosten. Cloud wird zwangläufig zum Massentrend. Egal ob für KMU oder Grossunternehmen. Der Trend hat unglaubliche Fahrt aufgenomen. Warum zögern? Die Antwort: Wer will schon seine lebenswichtigen Funktionen Dritten überlassen? Vertrauen ist nur mit IT Security zu gewinnen. Warum hat sich RMS von Microsoft anfänglich so schwergetan? Ganz einfach: Der Schlüsselaustausch findet in einem Key Exchange Container statt und dieser hatte eine Backdoor. Es hat 2 Jahre gedauert bis Microsoft begriff, das die Europäer da nicht mitmachen. MS musste dann nachgeben und hat Kunden zugestanden, Ihre eigenen Schlüssel mitzubringen.

Warum ist IT Security so komplex und schwierig: Wir liegen unter Anwendungen, oder darüber oder mitten drin. D.h. ein Security Experte muss alles und jedes IT Thema kennen. Das Wissen muss aussergewöhnlich tief und breit sein.
Jeden Tag lesen und hören wir über Break-ins, Hacking, Insider Theft of Data, und grossen angerichteten Schaden. Dazu kommt der Datenklaukrieg der IT Staaten, also der Chinesen, der Amerikaner, Israelis und Russen um nur die Grossen Akteure zu nennen. Hinzu gesellen sich Kriminelle Elemente, die jeden Tag cleverer und aggressiver werden. Wirtschaftsspionage findet im grossen Stil statt. Alles was Informationen verspricht wird attackiert und dazu ist jedes Mittel recht. Sie haben sicher über die Backdoors in den Chips von Intel und AMD usw. gelesen. Glauben Sie die Ursache sind einfache Fehler im Design? Intel und andere grosse Chip Hersteller machen keine Fehler. Dazu sind die QA Systeme zu gut. Nein, das war so gewollt um der NSA einfachen Zugang zu geben. Sie müssen wissen das die NSA jeder Zeit die Herausgabe von amerikanischen Schlüsseln durchsetzen können. Selbstverständlich findet der IT Krieg seit langem auf der Chip «embedded» Ebene statt. Es ist eine neue Form der Kriegsführung. Es geht um Daten von Produktionsprozessen, technische Entwicklungen und Forschung. Alles wird gestohlen. Daten zu hacken ist unendlich billiger als ein Projekt zu finanzieren. Jetzt stellen Sie sich vor was in der Cloud passiert ohne adäquate Sicherheit! Es ist schlichtweg furchterregend!
Früher bestimmten Betriebsprozesse IT Prozesse. D.h. IT passte sich an die Betriebsprozesse an. Heute kann man das nicht mehr so sagen. Heute bestimmt IT massgeblich wie die Prozesse ablaufen. Der Betrieb und IT passen sich

dynamisch an. Künstliche Intelligence und Cloud ändern auch die Rolle des CIO und des IT Key Management. Es wandelt sich in “shaping business processes instead of accommodating existing processes “. Zunehmend sehen wir IT Manager in der Chefetage was vor wenigen Jahre undenkbar war. CIO‘s waren als Experten mit Tunnelvision abgestempelt ohne das Zeug CEO zu werden. Heute könnte man sagen der CIO transformiert und ist der Chief Innovation Officer geworden. Eine viel bessere Bezeichnung für die Zukunft. Erinnern Sie sich: Nokia hatte 80% des mobilen Marktes in 2008. Erinnern Sie sich an Kodac. Was ist aus ihnen geworden. Viele andere Marken sind vom Markt verschwunden. Warum: Sie waren nicht in der Lage sich neu zu erfinden.

Business Management muss zwingend ein Bestandteil der Ausbildung sein. Im Zentrum muss die Fähigkeit stehen Ideen zu verkaufen. Ohne diese Fähigkeiten gibt es kein Geld bzw. Resourcen.
Job Garantien gibt es nicht mehr. Ohne Risiko gibt es keine Start-Ups. Ich sehe, dass man in der Schweiz meist auf Nummer sichergeht. Gute IT Leute wollen zu den grossen Firmen. Das ist für unsere Wirtschaft langfristig problematisch. Ich meine unser hiesiges StartUp Umfeld ist international nicht konkurrenzfähig. Es fehlt an Risikokapital und Menschen die hohe Risiken übernehmen. Wir haben so keine Chance gegen Silicon Valley zu konkurrieren. Sogar das viel kleinere Singapore bietet seit einigen Jahren bessere Bedingungen. Nur 1 von 10 Start-Ups überlebt. Jetzt startet Dubai durch und lockt mit viel Geld IT Start-Ups.
«Fear of failure» ist in Europa ein grosser Faktor der uns zurück hält. Wer bei uns Pleite macht ist abgestempelt als Verlierer. In den USA wird eine Pleite als Teil des «Reifens» gesehen. Wir müssen diese Einstellung ändern aber ich bin da leider skeptisch. Das hängt auch mit der Pleitegesetztgebung zusammen die es de facto unmöglich macht einem in Schwierigkeiten geratenem Unternehmen neues Leben einzuhauchen. Das ist mit Chapter 11 in den USA total anders. Deutschland hat die Gesetze angepasst und eine ähnliche Form der Restrukturierung geschaffen. Wo ist unsere Reform?
Zum Abschluss meiner Gedanken:
Wenn künstliche Intelligenz die Rakete ist, die uns in die nächste Revolution schiesst, sind es die DATEN die der Raketentreibstoff ist. Dies ist auch die Einsatzberechtigung für Halocore, welches Transparenz der SAP Daten bringt. Damit leisten wir einen wichtigen Beitrag zur nächsten digitalen Revolution.

SECUDE



Cybercrime in numbers

- **North Korean** and **Russian** hackers are most aggressive.
- Cyber attacks cost $ 600 Billion in 2017 versus
- 445 Billion in 2014

(McAfee and Center for Strategic & International Studies (CSIS).

- **Intellectual Property** (IP) theft accounts for about a quarter of the damage.
- White House announced last week that theft of IP in the USA in 2016 was between $56 and 109 Billion

A $155 billion increase over 2016

- Steve Grobman (McAfee): Cybercrime has become **efficient and very profitable**.
- James Lewis (Vice President, CSIS): **Russia dubiously ranks #1** in cybercrime due to hackers' skills and no law enforcement by Western nations possible.
- Followed by North Korea, which primarily targets digital currencies.
- **Iran** targets mostly financial institutions.
- China is focused on **espionage and IP**
- **Of course, the report does not state the IP theft of the USA on other countries and damage they cause.**

SECUDE