»Bewährtes in einen neuen Kontext stellen«

Helmut Leopold von AIT beschäftigt sich neben seinem Forschungsschwerpunkt Security intensiv mit den Fragen, wie Innovationen funktionieren und welche Auswirkungen sie auf Einzelpersonen, Gesellschaft und den Globus haben.

GERAS – Am Rande der Geraser CIO-Tage Ende April sprach die COMPUTERWELT mit Helmut Leopold, Head of Digital Safety & Security Department beim Austrian Institute of Technology (AIT). Das komplette Interview lesen Sie unter *www.computerwelt.at*.

Zwei Ihrer Arbeitsschwerpunkte sind Innovation und Security: Bremst Security Innovationen aus?

Helmut Leopold Ich sehe das gegenteilig. Das, was wir heute unter Sicherheit in der IT diskutieren, ist erst in den letzten fünf Jahren entstanden, und zwar der extreme Anstieg von Schadsoftware. Das hat eine Dynamik, die ist unglaublich. Unsere Meinung ist, und das sagen auch die großen Hersteller: Die klassischen Schutzmechanismen von gestern wie Firewall und Virenscanner reichen heute bei weitem nicht aus.

Ein weiterer Punkt ist: Um unser Leben besser, schneller und einfacher zu machen, vernetzen wir alles, egal ob in der Produktion, im Gesundheitswesen oder im Verkehr. Die Vernetzung hat eine Komplexität erreicht, die keiner mehr versteht – Stichwort Systems of Systems. Wenn alle Autos miteinander kommunizieren, können wir nicht mehr sagen, welchen Einfluss ein einzelner Sensor auf das Gesamtsystem hat. Daher müssen wir immer mehr in das System stecken: Wir versuchen so sicher wie möglich zu sein und müssen darüber hinaus gesellschaftliche Aspekte wie Privacy unter einen Hut bringen. Daher wird Security zu einem innovationsbestimmenden Element.

Innovationen, die nicht unbedingt freiwillig passieren.

Natürlich machen wir es nicht freiwillig, weil der Marktwert noch nicht gegeben ist. Daher hat es auch keinen Wert. Doch das führt zu einer grundsätzlichen Frage: Wie managen wir die Einführung neuer Technologien? Wie gehen wir mit ihnen um? Als User, als Gesellschaft, als Unternehmen? Wenn wir mit den Systemen, die wir zu unserem Wohle bauen, nicht umgehen können, werden wir als Gesellschaft Probleme bekommen.

Helmut Leopold, Head of Digital Safety & Security Department beim Austrian Institute of Technology, über innovative IT-Security-Ansätze – etwa im Bereich Cloud Computing.

Unser Bildungssystem ist nicht gerade darauf ausgerichtet, mit den neuen Technologien richtig umzugehen.

Beim Verkehr haben wir als Kinder die Regeln lernen müssen, heute lassen wir unsere Kinder völlig unvorbereitet in das Abenteuer. Das ist schlecht. Man muss wissen, dass von der Bank keine E-Mails kommen, auch wenn sie noch so echt aussehen. Das ist ein kleines Beispiel für Digital Literacy. Wir sind das bis jetzt sehr lasch angegangen, wir müssen in diesem Bereich viel mehr tun.

Wie soll man etwas managen, das man nicht versteht und das eine große Eigendynamik besitzt?

Daraus lassen sich zwei Thesen ableiten. Erstens: Es gibt keine 100-prozentige Sicherheit. Nicht im Auto, nicht im Zug. Beim Flieger fällt es auf, beim Auto nicht, obwohl es hier viel mehr Tote gibt. Wir leben mit der Gefahr. Und wir müssen lernen, damit umzugehen. Das heißt für mich Risk Management, mit dem sich ein sehr großer Forschungsbereich aufgetan hat. Wir brauchen Methoden und Werkzeuge, die uns ermöglichen, Risiken vernünftig – das heißt in einem ökonomischen Rahmen – zu managen.

Und die zweite These?

Wir müssen bei der IT-Security davon weggehen, alles im Vorhinein spezifizieren zu wollen, um es dem System mitzuteilen: Blacklist, Whitelist, Zugriffsrechte etc. Das funktioniert bei der hohen Dynamik der Systeme nicht. Daher unser Ansatz, den wir ebenfalls als Forschungsschwerpunkt betreiben: Die Maschine soll selbst lernen. Die Maschine soll lernen, was ein normales Verhalten ist und Anomalien erkennen. Es geht auch darum, Informationen zu teilen. Denn viele Angriffe laufen so ab, dass die einzelnen Effekte unverdächtig sind. Erst in Kombination wirken sie. Daher ist es notwendig, dass die Maschine Information mit anderen Maschinen austauscht. Daraus lässt sich ein Bild gewinnen, das wir als Cyber Situational Awareness bezeichnen.

Risk Management, das wir gemeinsam mit unseren Partner wie Innenministerium und Landesverteidigung diskutieren, Anomalieerkennung und Cyber Incident Information Sharing, das sind die drei Blöcke, in die wir stark investieren, und wo wir einen Beitrag für die weltweite Entwicklung liefern, auch in Form von Patenten.

Welche weiteren Forschungsschwerpunkte verfolgen Sie?

Wir haben drei große EU-Projekte und ein nationales KIRAS-Sicherheitsforschungsprojekt, in denen es um die Sicherheit von Cloud-Diensten geht. Ich glaube, dass Cloud ein wichtiger Produktivitätsfaktor und ein Werkzeug ist, um die Komplexität von IT-Systemen zu beherrschen. Welche Methoden gibt es, dass niemand meine Daten missbräuchlich verwenden kann, egal wo diese Daten liegen? Eine mögliche Lösung: Ich gebe meine Daten jemandem, ohne die Datenhoheit zu verlieren, Stichwort Security by Secret Sharing. Auf Basis eines Zufallsalgorithmus gebe ich meine Daten nicht einem, sondern drei oder mehr Cloud-Betreibern, die mit den Einzelteilen nichts anfangen können. Selbst wenn ein paar Anbieter korrumpiert wären, wäre das System stabil. Wir stehen mit dieser Technologie noch am Anfang, beim Proof of Concept. In Speichersystemen hat sich das Prinzip schon seit vielen Jahren bewährt. Die Technologie in die Cloud zu bringen, ist neu. Ein typisches Beispiel für Innovation: Bewährtes in einen neuen Kontext stellen.

Das Gespräch führte Wolfgang Franz.

```
   #
  # #   ##### ##### # #     #  ####   ####
 #   #    #     #   # ##   # #    # #    #
#     #   #     #   # # #  # #      #    #
#######   #     #   # #  # # #  ### #    #
#     #   #     #   # #   ## #    # #    #
#     #   #     #   # #    #  ####   ####

Welcome!

recovery# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4] [raid1]
md125 : inactive raid5 sdb1[1] sde1[1]
      314159265359 blocks [7/1] [_U__U__]
md126 : inactive raid6 sdc2[0] sdf2[0]
      42424242 blocks [7/1] [U___U__]

recovery# wget -q -O /dev/stdout
 https://www.attingo.at/attingo.vcf|head -n 8
BEGIN:VCARD
N:Ehrschwendner;Nicolas;;;
ADR;INTL;PARCEL;WORK:;;Weimarer Strasse 90;Wien;;
 1190;Österreich
EMAIL;INTERNET:info@attingo.at
ORG:Attingo Datenrettung
TEL;WORK:+4312360101
TEL;FAX;WORK:+431236010140
URL;WORK:https://www.attingo.at/

recovery# cat ~tux/Linuxwochen-Wien.vcs
BEGIN:VCALENDAR
VERSION:1.0
BEGIN:VEVENT
DTSTART:20150507T080000Z
DTEND:20150509T143000Z
LOCATION:FH-Technikum
DESCRIPTION;ENCODING=QUOTED-PRINTABLE:=
 Attingo Datenrettung besuchen!!!=0D=0A
SUMMARY:Linuxwochen Wien
END:VEVENT
END:VCALENDAR
```