Ausbildung für «Geeks»: In Australien wird IT-begabten Schülern auch Management- und Sozialkompetenz beigebracht.

Bild: Monte Rego Images/ Shutterstock

Ein Umdenken tut not

Cybergefahren verlangen beides: Selbstverantwortung und verstärkte Zusammenarbeit. Weitermachen wie bisher wäre gefährlich und fahrlässig. Ein wichtiger Schlüssel zum Erfolg ist die Verbreitung von Wissen, Verständnis und Know-how. **Von Reinhard Riedl ***

Die Gefahr lauert überall und sie ist sehr real. Schon nagelneue, frisch ausgelieferte Smartphones, die noch nie benutzt wurden, können mit feindlicher Software verseucht sein. Wenn aber Geräte erst einmal am Netz sind, dann kommt die Gefahr von allen Seiten. Trotzdem passiert wenig – oder scheint wenig zu passieren. In der Öffentlichkeit wird nur alle paar Monate ein grösserer Fall von Cyberkriminalität bekannt und kaum einer hört von einem Vorfall in der eigenen Organisation. Das wirft die Frage auf: Sind Cyberkriminalität, Cyberkrieg und Cyberterrorismus nur Ammenmärchen?

Vom Militär hört man oft, dass unsere Feinde an den Grenzen stehen. Das stimmt nicht. Grenzen gibt es in der virtuellen Welt gar nicht. Wenn, dann sitzen unsere Feinde in unserer Küche und im Wohn- und Schlafzimmer – oder auch in der Kamera, die zwecks Sicherheit unseren Garten bezüglich verdächtiger Bewegungen überwacht. Im virtuellen Raum geht es nicht um die Verteidigung von Landesgrenzen, sondern um die Verteidigung von Rechten und Ansprüchen – zu allererst des Rechts auf Privatsphäre und des Schutzes von Eigentum. Darüber hinaus aber auch des Rechts auf Teilnahme am wirtschaftlichen und sozialen Online-Leben. Die wachsende Bedrohung dieser Rechte und Ansprüche ist ein sehr reales Problem und stellt ein reales Risiko dar, das engagiertes Handeln verlangt, weil die möglichen Folgen so schwerwiegend sind.

Dabei gibt es einige grundsätzliche Herausforderungen, die daher kommen, dass im virtuellen Raum andere Spielregeln gelten und eine andere Verhaltenskultur vorherrscht als in der physischen Welt:

- **Sozialer Schutz:** Die natürlichen Hemmnisse für kriminelles Handeln sind wesentlich geringer, weil es oft keine soziale Kontrolle gibt: Niemand kann beispielsweise dem Internetdieb beim Stehlen zuschauen, ohne Spezialwerkzeuge und besondere Fachkenntnisse zu nutzen. Und kaum einer kann anderen helfen, wenn sie Opfer werden.

- **Selbstschutz:** Der Selbstschutz ist anspruchsvoller als in der physischen Welt und muss speziell erlernt werden. Dazu gehört neben dem präventiven Schutz insbesondere die Fähigkeit, frühzeitig zu erkennen, wenn man Opfer eines Verbrechens wurde, um vernünftig darauf zu reagieren.

- **Kriminelle Möglichkeiten:** Kriminelle Akteure können sehr effizient viele gleichzeitig angreifen, weil die Notwendigkeit zur Anwesenheit vor Ort nicht besteht. Ausserdem haben sie viele Optionen, aus gänzlich verschiedenen Richtungen über ihre Opfer herzufallen.

- **Entgegengesetzte Paradigmen:** Bei der Geräteproduktion wünscht man sich geschlossene Produzentenkreise im eigenen Land. Bei der Früherkennung und der Reaktion im Desasterfall bräuchte es eine offene Zusammenarbeit. Ersteres ist angesichts der Marktdominanz amerikanischer IT-Unternehmen illusorisch, Zweiteres widerspricht konventioneller Sicherheitslogik und individuellen Machtinteressen. Beides passt nicht gut zusammen.

- **Fehlende Standards:** Kriminelle und feindselig agierende Staaten profitieren davon, dass es keine einheitliche Rechtsverfolgung gibt und dass auf der operativen Ebene die Zusammenarbeit schwierig ist (während sie auf technischer und auf strategischer Ebene einfacher realisiert werden kann).

Die politische Perspektive

Dazu kommt die demokratische Komponente. Ist die Schweiz in vielen Jahrhunderten nicht gut gefahren damit, dass die Gemeinschaft vom Einzelnen Eigenverantwortung und Engagement für die Gemeinschaft einfordert? Haben nicht gerade das Selbstverantwortungsprinzip und die Freiwilligenarbeit zu einem vernünftigen Staat geführt, dessen Behörden im öffentlichen Interesse handeln statt (wie anderswo) im Interesse ihrer Mitarbeiter und der herrschenden Eliten?

Eine erfolgversprechende Antwort auf die Herausforderungen kann deshalb nicht lauten, dass wir top-down von Staatsstellen umfassend geschützt werden. Sie kann aber auch nicht in der Aufforderung bestehen, dass jeder allein für sich selber Sorge tragen muss. Denn in dieser Situation sieht sich jeder von uns einer Übermacht von fremden Staatsinteressen und kriminellen Energien gegenüber. Stattdessen braucht es ein demokratisch gesteuertes staatliches Engagement, das freiwilliges Engagement von Fachkundigen einbindet und auch die Befähigung zum Selbstschutz beinhaltet. Letztere beginnt bei der Weiterbildung der Lehrer, damit diese im Unterricht die Grundlagen legen können – angefangen in der Primarschule.

Wir alle müssen lernen mit der Gefahr zu leben – und zum wir gehören auch unsere Institutionen. Das fordert ein Miteinander von Eigenverantwortung und staatlichem Engagement, ebenso wie ein konstruktives Nebeneinander von Zusammenarbeit und Offenheit einerseits und geschlossenen, sicheren Produktionszyklen anderseits. Ein Umdenken und Andersdenken stellt hier eine grosse Chance dar, den eigenen Handlungsspielraum zu vergrössern.

Down Under ganz anders

Ein eindrückliches Beispiel für so ein Andersdenken liefert ein Besuch am Cybersecurity Lab der University of New South Wales (UNSW). Die Australier nehmen das Thema viel ernster als die Europäer. Neben einem eigens zuständigen Minister, einem eigenen, hochqualifizierten Beraterstab für den Regierungschef und einer grossen nationalen Konferenz investieren sie auch beträchtlich in Aus- und Weiterbildung. Und das tun sie anders als wir.

Die Ausbildungsstrategie im Cybersecurity Lab der UNSW zielt darauf ab, zukünftige Cybersecurity-Manager auszubilden, die fachlich hochkompetent sind, weil sie zu Beginn ihrer Karriere Cybersecurity «Geeks» waren. Jungen Männern – das Problem, wie man mehr Frauen für Informatik begeistert, haben die Australier auch noch nicht gelöst –, die schon in der High School ihre Lehrer mit Fachwissen terrorisierten, wird Teamarbeit und managementtaugliches Selbstmarketing beigebracht. Die Universität fördert gleichzeitig ihr Fachwissen und ihre soziale Intelligenz. Das Ergebnis ist, dass die Studierenden nicht nur viele Hacker-Preise einheimsen, sondern danach auch Karriere im Management machen. Der resultierende Nutzen für die Wirtschaft und letztlich die Gesellschaft ist, dass es im höheren IT-Management Cybersecurity-Fachspezialisten gibt. Das ist ein hoher Wert für das Gemeinwohl.

Jeder braucht Expertise

Das australische Beispiel weist in die richtige Richtung: Es geht darum eine Wissensbasis im System zu verankern und Cybersecurity-Expertise mit anderen Expertisen zu vernetzen: Von den Software-Entwicklern bis zur Geschäftsleitung sollten alle Cybersecurity-Fachwissen besitzen. Das hilft doppelt: Zum einen handeln alle in ihren Wirkungskreisen vernünftiger und zum anderen wird das Beschliessen und Umsetzen vernünftiger Massnahmen erleichtert. Denn ein ausschliessliches Delegieren der Probleme an Experten funktioniert bei Cybersecurity-Problemen nicht.

Für Gemeinden heisst dies dreierlei: Sie müssen selber Cybersecurity-Expertise aufbauen, allenfalls im Verbund von mehreren Gemeinden. Sie sollen vom Kanton dabei einfordern, dass er den Wissensaustausch fördert. Und sie können durch ihre Beteiligung am Austausch aktiv zum Schutz der Schweiz beitragen. ■

*** Reinhard Riedl** ist Leiter des BFH-Zentrums Digital Society. Er war bis 2014 Leiter des E-Government-Instituts der Berner Fachhochschule.

Berner Fachhochschule

Das BFH-Zentrum Digital Society beschäftigt sich mit den Chancen und Risiken der digitalen Transformation von Wirtschaft und Gesellschaft. Es entwickelt praxistaugliche Lösungen basierend auf aktuellen Forschungsergebnissen. Dabei setzt es auf die Analyse von Praxisbeispielen in ganz Europa und auf die experimentelle Entwicklung und Pilotierung neuer Lösungskonzepte.

Als Partner des Kommunalmagazins verfassen Mitglieder des BFH-Zentrums Digital Society in jeder Ausgabe einen Artikel zum Thema Digitalisierung und Gemeinden.

Einer der sechs Schwerpunkte des BFH-Zentrums Digital Society ist «Cybersecurity und IT-Forensik». Aktuell wird in diesem Schwerpunkt insbesondere zu E-Voting geforscht, aber auch der Bau von sicheren, hochperformanten Blockchains ist ein Forschungsthema. Diese Blockchains können unter anderem im Gesundheitswesen und in der Finanzwirtschaft eingesetzt werden.

Veranstaltungshinweise

Wrestling with the Algorithm:
Konzert und Podiumsdiskussion am 14. Oktober, 19.30 bis 21.30 Uhr im Progr in Bern. *www.ignm-bern.ch*

«eGov Fokus»: «Good Moooooorning Switzerland!» – Wie geht erfolgreiche Projektabwicklung in der öffentlichen Verwaltung?:
10. November, 9.00 bis 16.15 Uhr im Berner Rathaus.
www.e-government.bfh.ch/egf

11. E-Government Symposium Schweiz:
13. November, 12.30 bis 21.00 Uhr im Hotel Bellevue in Bern.
www.egovernment-symposium.ch