FDP
Die Liberalen

FDP. Die Liberalen Unterägeri und Oberägeri

Öffentlicher Anlass - Cyber Security / Interview mit Ständerat Joachim Eder

Am **Dienstag, 22. Mai 2018, 19:30 Uhr** findet in der AEGERIHALLE in Unterägeri ein öffentlicher Anlass zum Thema Cyber Security statt, gemeinsam organisiert durch die beiden FDP Ortsparteien im Ägerital. Namhafte Persönlichkeiten werden in 4 Kurzreferaten mit anschliessender Podiumsdiskussion den aktuellen Stand der Sicherheit im Internet in der Schweiz und vertieft im Kanton Zug aufzeigen.

Kurzreferate und Podiumsteilnehmer:
Joachim Eder Ständerat, Unterägeri
Giuliano Otth CEO Crypto Schweiz AG, Steinhausen
Thomas Armbruster Kripochef Zuger Polizei
Mike Tonazzi CEO tonazzi dot net ag, Rotkreuz

Moderation Podiumsdiskussion:
Andreas Kleeb, Beelk Group

Zur Einstimmung ins Thema führte René Kley, Vizepräsident der FDP Unterägeri, mit Ständerat Joachim Eder am 1. Mai 2018 das nachfolgende Interview:

Wieso müssen wir uns mit Cyber-Security auseinandersetzen?

Der Zuger FDP-Ständerat Joachim Eder engagiert sich schon länger aktiv für das Thema Cyber-Security. Seine im Juni 2017 eingereichte Motion zur Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund wurde, gegen den Widerstand des Bundesrates, mit wenigen Gegenstimmen angenommen.

1. Alle reden über Cyberkriminalität, Cybermobbing oder die Abwehr von Cyberangriffen. Woher kommt der Begriff „Cyber“ eigentlich?

Der Begriff Cyber kommt aus dem Altgriechischen und bedeutet Steuerung und wurde als Synonym für das Navigieren in der Schifffahrt verwendet. In den 70Jahren war Cyber der Markenname eines Grosscomputers. Dieser war zu dieser Zeit der leistungsstärkste digitale Rechner der Welt. Mittlerweile bringt man den Begriff in Verbindung mit dem englischen Cypernetic, wiederum ein Synonym der vernetzten Datenwelten im Internet. Cyberkriminalität, Cyberattacken sind Manipulationen in der Datenwelt des Internet, die ohne das Wissen der Betroffenen fremdgesteuert ablaufen.

2. Was sind aus deiner Sicht heute die grössten Risiken im „Cyber-Raum“?

Das Typische an der Cyberthematik ist, dass es keine Grenzen gibt. Keine Kantonsgrenzen, keine Landesgrenzen, man kann von überall her via Internet auf alle vernetzten Computer der Welt zugreifen. Dies ist ziemlich problematisch, weil man die Vernetzungen und die damit verbundenen Zugriffe auf Computer und deren Daten nicht sieht. Täglich finden in der Schweiz 1000nde Attacken auf Computersysteme statt. Wenn alle Attacken publiziert würden, wären die Zeitungen voll von entsprechenden Nachrichten. Unternehmen wie auch Behörden, die von einer Cyberattacke betroffen sind, publizieren diese in der Regel nicht. Eine Ausnahme war der Fall RUAG. Als Rüstungsbetrieb bestand bei der RUAG ein öffentliches Interesse zur Aufklärung. Die RUAG wollte einem Imageschaden vorbeugen und mögliche Zweifel, dass das Unternehmen die Cyberrisiken nicht angemessen eingeschätzt haben könnte, ausräumen. Angriffe auf kritische Infrastrukturen wie die Energieversorgung, Banken, Spitäler oder militärische Einrichtungen sind meines Erachtens die grössten Risiken. Ein Beispiel dafür ist das amerikanische Gesundheitswesen. In den Spitälern müssen die Patienten ihre Kreditkartendaten für die Zahlungsmodalitäten angeben. Weil die Personendaten zusammen mit den Kreditkarteninformationen für kriminelle Organisationen oder Hacker äusserst attraktiv sind, ist das Risiko eines Cyberangriffes besonders hoch einzuschätzen. Diese Risikoeinschätzung müsste diese Institutionen dazu veranlassen, entsprechende Sicherungsmassnahmen einzusetzen, um einen Datenabfluss zu verhindern.

3. Wer steht hinter diesen Cyberattacken und welche Ziele verfolgen die Initianten?

Einzelpersonen oder Gruppen mit grossem Informatikfachwissen wollen die Schwächen im Cyberraum ausnützen. Der Missbrauch von geschützten Daten für kriminelle oder terroristische Aktivitäten steht dabei

im Vordergrund. Je nach dem können auch staatliche Interessen und Geheimdienstaktivitäten hinter einem Cyberangriff stehen. So ist der bereits erwähnte Angriff auf das Schweizer Rüstungsunternehmen RUAG von Russland ausgegangen, dies konnte in der Zwischenzeit festgestellt werden. Es ist eine neue Dimension der Kriegsführung, weg vom Erd- oder Luftkampf, hin zum nicht oder schwer kontrollierbaren Informations- und Datenkrieg im Cyber-Raum. So ist es meines Erachtens wenig nützlich, wenn wir beste Flieger und eine gut ausgestattete Luftabwehr haben, aber nichts oder zu wenig machen um uns gegen die Bedrohungen im Cyber-Raum zu schützen.

Es muss alles daran gesetzt werden, dass wir unsere kritischen Infrastrukturen auf privater wie auch auf staatlicher Ebene optimal schützen. Kein attraktives Ziel für die Angriffe aus dem Cyber-Raum darzustellen, sollte unser oberstes Ziel sein. Der Angriff auf die Datenbank des Deutschen Bundestages 2015, von dem man heute noch nicht weiss, wer dahintersteckte, ist ein anschauliches Beispiel, welche Dimensionen Angriffe im Internet annehmen können.

4. Welche Massnahmen kann ein KMU oder eine Privatperson ergreifen, um das Risiko, Opfer eines Cyberangriffs zu werden, klein zu halten?

Cyberangriffe haben ja verschiedene Gesichter, Systeme können gehackt werden oder über Einzel-Computer werden Viren gestreut. Diese Angriffe können auch in KMU's und bei Privatpersonen und nicht nur bei grossen Infrastrukturen Schaden anrichten. Das Entscheidendste ist, dass wir das Internet und die Informatikmittel bewusst und mit der gebotenen Vorsicht nutzen. Der sorglose Umgang mit den Informatikmitteln ist das grösste Risiko, das es zu vermeiden gilt. Ich erhalte auch E-Mails von Absendern, die täuschend echt wirken und in denen ich aufgefordert werde, einen Link oder ein Dokument im Mailanhang zu öffnen. Dementsprechend ist auch der Schutz der eigenen Hard- und Software mit Schutzeinrichtungen wie Firewall und aktuellem Virenschutzprogramm sehr wichtig. Die regelmässige Datensicherung (Backup) ist ebenfalls unabdingbar. Nur wenn man diese Verhaltensregeln beachtet, reduziert sich das Risiko, Opfer eines Cyberangriffes zu werden. Die Daten meines „Parlamentarier-Laptops" werden von MOUNT10 im SWISS FORT KNOX gelagert. Diese Sicherheitsmassnahme gibt mir ein gutes Gefühl. Nicht zu unterschätzen sind auch die Aktivitäten in den Social-Media-Kanälen – ich bin ein bekennender Social-Media-Abstinenzler – bei denen enorme Mengen an zum Teil sehr persönlichen Daten und Bildern in kriminelle Hände kommen können.

5. Trotz guten Vorkehrungen und der Einhaltung von Datensicherheit und Datenschutz, gibt es keine 100%ige Sicherheit im Internet!
Was kann bzw. muss bei einem Cyberangriff getan werden?

Auf keinen Fall bei einem Angriff mit einer Zahlungsaufforderung etwas bezahlen. Es wird auch immer wieder darauf hingewiesen, dass Dienstleistungsbetriebe wie Banken, Kreditkarteninstitute oder Versicherungen ihre Kundenkontakte nicht über den ungeschützten Mailverkehr pflegen. Die Betroffenen, auch Privatpersonen, sollen sich bei MELANI, der Melde- und Analysestelle Informationssicherung melden. Diese vom Bund eingerichtete Stelle gibt Auskunft, was bei einem Cyberangriff zu tun ist. Als KMU oder Privatperson ist der Zuzug von IT Fachpersonen angezeigt. Ziel muss es sein, den Angriff zu lokalisieren und die Weiterverbreitung von Computerviren zu verhindern. Einem KMU würde ich empfehlen, eine minimale IT-Sicherheitsstrategie inklusive dem Vorgehen zur Datenwiederherstellung bei einem möglichen Schadenfall zu formulieren. Als Sofortmassnahme bei einem Schadenereignis hat sich das sofortige Trennen der Computeranlage von der Stromzufuhr und das Ausschalten des WLAN bewährt. Fachpersonen sollten dann infizierte Systeme analysieren und die Massnahmen zur Wiederinbetriebnahme mit den Betroffenen besprechen. In gravierenden Fällen würde ich sogar Anzeige gegen Unbekannt erstatten.

6. Aktuell will der Bund das System zur Erfassung biometrischer Gesichtserkennungs- und Fingerabdruck-Daten für Schweizer Pässe ersetzen. Dafür kommen Privatfirmen in Frage, möglicherweise auch ausländische Firmen.
Wie stehst du zu einer möglichen Auftragsvergabe an ausländische Firmen?

In diesem Zusammenhang erscheint mir die Unterscheidung in ausländische und schweizerische Firmen zu einfach. Viele Schweizer Firmen beschäftigen Mitarbeitende aus dem Ausland. Angenommen, der Auftrag würde an ein solches Unternehmen vergeben, macht dies meines Erachtens keinen Unterschied zu einer Auftragsvergabe an ein ausländisches Unternehmen. Wichtig erscheint mir in diesem Zusammenhang viel mehr, dass klare Rahmen- bzw. Auftragsbedingungen festgelegt sind. Beim Bund kennen wir unter anderem die Personensicherheitsprüfung, die sehr umfassend ist. Alle Personen, die in sicherheitsrelevanten

Prozessen und Funktionen tätig sind, müssen diese Prüfung durchlaufen. Aus meiner Sicht ist der grösste Risikofaktor immer der Mensch und dies unabhängig ob mit oder ohne Schweizer Pass. Auch die mögliche Auftragsvergabe an ein Unternehmen mit Sitz im Ausland sollte gleich behandelt werden. Bereits bei der Ausschreibung von Projekten und Aufträgen, insbesondere bei einer solchen Ausschreibung, müssen die Vergabekriterien den Anforderungen entsprechend festgelegt werden. Dies um sicherzustellen, dass nur qualifizierte, vertrauenswürdige und fachlich versierte Unternehmen eine Chance haben die Ausschreibung zu gewinnen. Sicher würde ich es begrüssen, wenn ein Schweizer Unternehmen in Zukunft diese Aufgabe übernehmen würde. Die mögliche Auftragsvergabe ins Ausland birgt unbestritten auch ein politisches Risiko. Diese Thematik hatten wir ja bereits im Kanton Zug, als der Auftrag für das Einscannen der Zuger Steuererklärungen auswärts vergeben wurde. Der politische Druck hat die Steuerverwaltung dazu veranlasst, diesen Auftrag wieder zurückzunehmen.

7. Im Stände- wie auch im Nationalrat wurde die von dir Mitte 2017 eingereichte Motion zur Schaffung eines Cyber-Security-Kompetenzzentrums, gegen den Widerstand des Bundesrates, mit wenigen Gegenstimmen angenommen.
An was würde ein KMU oder eine Privatperson merken, dass dieses Cyber-Security-Kompetenzzentrum die Arbeit aufgenommen hat und gute Arbeit leistet?

Im letzten Monat hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 verabschiedet. Gemeinsam mit der Wirtschaft, den Kantonen und den Hochschulen soll nun aufgezeigt werden, mit welchen Massnahmen den Cyber-Risiken begegnet werden kann. Zu diesen Massnahmen gehört auch das Einrichten eines Cyber-Security-Kompetenzzentrums. Zurzeit wird darüber gestritten, in welchem Departement dieses angesiedelt werden soll! Für mich ein typisches Beispiel dafür, dass wir in unserem Land noch erhebliches Potential haben, besser zusammenzuarbeiten, um gemeinsame und wichtige Themen zu koordinieren. Eine der Hauptstossrichtungen meines Anliegens ist ja, dass alle mit dem Cyber-Raum zusammenhängenden Aktivitäten koordiniert sind. Heute nimmt diese Rolle die Melde- und Analysestelle Informationssicherung MELANI wahr. MELANI leistet sehr gute Arbeit, hat aber aktuell zu wenig Ressourcen für aktive Koordinationsaufgaben zwischen den Bundesstellen, den Kantonen und der Wirtschaft. Mit der ETH Zürich und der EPFL Lausanne haben wir zwei “Leuchttürme“ in der Schweiz, die Informatikfachpersonen in den verschiedensten IT-Disziplinen ausbilden. Erst wenn auch unsere Wissenschaft verbindlich in diese Thematik eingebunden ist, sind wir einen beträchtlichen Schritt weiter. Aktuell ist nicht zu überblicken, welche und wie viele Akteure sich mit diesem Thema beschäftigen. Der Bürger oder ein KMU spürt den Erfolg dann, wenn das Thema Cyber-Security ein Gesicht hat. Ein Gesicht, das in der Öffentlichkeit wahrgenommen wird und sich auch in der internationalen Zusammenarbeit profiliert.