

**FRANZ GRÜTER** – Der Luzerner SVP-Nationalrat und Verwaltungsratspräsident der green.ch AG sieht in Sachen IT-Sicherheit noch Handlungsbedarf bei den Unternehmen und in der Politik.

# «Jetzt die Weichen stellen»

**Schweizerische Gewerbezeitung:**  
Wie steht es um die IT-Sicherheit in der Schweiz?

■ **Franz Grüter:** Es besteht sicherlich Handlungsbedarf. Wenn man die jüngsten Angriffe mit Verschlüsselungstrojanern oder DDoS-Attacken analysiert, wird schnell klar, dass das ein lukratives Business für kriminelle Akteure ist. Ich nehme daher an, dass die Angriffe eher zunehmen werden.

Wo sehen Sie die grössten Gefahren für KMU?

■ Die Gefahren sehe ich bei KMU vor allem bei der Zunahme der Erpressungsversuche, sei es dadurch, dass Systeme verschlüsselt und blockiert werden oder die Website lahmgelegt wird. Dabei gehen die Täter immer professioneller vor, Trojaner werden aufwendig getarnt, die Opfer ausspioniert und mittels falscher Identitäten zu bestimmten Handlungen motiviert. Beim Trojaner Petya, der sich kürzlich verbreitete, wurde die Schadsoftware gar in einem Software-Update versteckt. Das macht es immer schwieriger für KMU, die Attacken zu erkennen.

Was müssen KMU tun, um sich gegen Hackerangriffe zu schützen?

■ Das ist von der Form des Angriffes abhängig. Sicherheit bei den E-Mails ist wichtig, die Website und der Online-Shop sollten vor DDoS-Attacken geschützt werden, und das Unternehmensnetzwerk und die Internetanbindung müssen richtig aufgebaut werden. Neben diesen gängigen Massnahmen sollten KMU sich Zeit nehmen, um das Thema IT-Sicherheit und -Verfügbarkeit ganzheitlich zu betrachten.

An welche organisatorischen Massnahmen denken Sie da?

■ IT-Sicherheit im Unternehmen betrifft jeden einzelnen Mitarbeitenden. Je besser die Anwender geschult sind, desto weniger tappen sie in die gängigen Fallen. Zudem empfiehlt es sich, die Risiken im Unternehmen periodisch zu überprüfen und auch Notfallszenarien durchzuspielen. In der Realität funktioniert manches anders als auf dem Papier.

Woran denken Sie hier konkret?

■ Es nützt wenig, wenn mein Netzwerk durch Firewalls bestens ge-



«Ich persönlich bin sehr konsequent darin, meine Geräte immer auf dem aktuellsten Stand zu halten und meine Daten regelmässig zu sichern», sagt Franz Grüter, Verwaltungsratspräsident der green.ch AG.

BILD: KEYSTONE/GAETAN BALLY

schützt ist, aber der Server bei einem Stromunterbruch nicht mehr erreichbar ist und ich keinen Zugriff mehr auf wichtige Daten und Programme habe. IT-Sicherheit und -Verfügbarkeit bedeutet, sich darüber Gedanken zu machen, wie die Systeme betrieben werden, wie man Ausfälle und Unterbrüche verhindert.

Und wie halten es die KMU mit dem Unterhalt ihrer IT?

■ Ganz unterschiedlich. Sie sind sensibilisiert, was die Gefahren betrifft und haben oft schon Massnahmen umgesetzt. Gut funktioniert das Updates und Patches der Software oder auch der Virenschutz. Das Fachwissen im Bereich Datensicherung, bei den Netzwerkeinstellungen oder auch bei organisatorischen Massnahmen der IT-Sicherheit wäre aber ausbaubar. KMU verfügen nicht immer über genügend internes Fachwissen und sind dann auf externe Hilfe angewiesen.

Was raten Sie KMU, wenn es um die Datensicherung geht?

■ Eine regelmässige und mindestens tägliche Datensicherung ist für jeden Betrieb Pflicht. Das sollte so einfach wie möglich, am besten automatisch gesteuert, geschehen. Je komplexer das Sichern wird, desto seltener wird es gemacht. Das stelle ich in Gesprächen mit kleineren Betrieben immer wieder fest. Wenn noch physisch gesichert wird, muss die Sicherungskopie an einem anderen Standort aufbewahrt werden. Wer einen Cloud-Dienst nutzt, braucht sich darum nicht zu kümmern.

Wie schützen Sie sich selber und die Daten Ihrer Kunden vor Hackern?

■ Informationssicherheit wird eigentlich immer auf zwei Ebenen erzielt: durch organisatorische sowie durch technische Massnahmen. Das heisst konkret: Jeder Mitarbeitende muss die wichtigsten Verhaltensregeln der IT-Sicherheit kennen, und es braucht technische Komponenten, die vor Angriffen schützen resp. diese abwehren. Ich persönlich bin sehr konsequent darin, meine Geräte immer auf dem aktuellsten Stand zu halten und meine Daten regelmässig zu sichern.

Rechenzentren in der Schweiz wachsen so stark wie in keinem anderen europäischen Land. Weshalb gerade hier?

■ Die Schweiz bietet Standortvorteile, die für die Betreiber attraktiv sind. Die Schweiz gilt als sicher und stabil, verfügt über sehr gute Infrastrukturen, eine bezahlbare und stabile Energieversorgung und bestens ausgebildete ICT-Fachkräfte auf allen Stufen. Die Schweiz weist hinter Irland die zweithöchste Rechenzentrumsdichte in Europa auf – die Standortvorteile sprechen also scheinbar für eine Datenunterbringung in der Schweiz, auch ausländische Unternehmen kommen hierher. Hinzu kommt, dass immer mehr Unternehmen ihre IT auslagern. Der Betrieb eigener Serverräume ist zu teuer geworden, da die Anforderungen an die Datenverfügbarkeit gestiegen sind.

**«IN DER REALITÄT FUNKTIONIERT MANCHES ANDERS ALS AUF DEM PAPIER.»**

Sensible Daten werden oft in alten Bunkern tief im Berg aufbewahrt. Lebt hier der Reduit-Gedanke wieder auf?

■ Solche Bunker gibt es tatsächlich. Für die meisten Unternehmen ist ein schwer zugänglicher und abgeschotterter Bunker für die Unternehmensinformatik aber nicht ideal. Immerhin müssen Techniker Hardware warten und der Datenaustausch mit dem Unternehmenssitz muss zeitnah über kurze Wege erfolgen können. Sicherheit lässt sich heute mit modernen Schutzmassnahmen mindestens ebenso effektiv in extra konstruierten neuen Rechenzentren erreichen. Aber für den Ruf des «Datenbunkers» Schweiz sind diese Rechenzentren natürlich förderlich.

Die von green.ch betriebenen Rechenzentren befinden sich im Wirtschaftsraum Zürich, das neuste in Lupfig im Aargau. Was hat Sie dazu bewogen, dort zu investieren?

■ Wir haben während eines Jahres den Standort für unser neuestes Rechenzentrum evaluiert. Die sichere Lage, die gute Erreichbarkeit und eine gute Strom- und Glasfaser-Anbindung waren entscheidend für uns. Zudem wollten wir möglichst nah an den Wirtschaftszentren bauen, um für möglichst viele Unternehmen das Haupt- oder Zweitrechenzentrum betreiben zu können.

Ab welcher Betriebsgrösse macht es für eine Firma Sinn, ihre Daten auszulagern?

■ Das macht bereits für kleinste Unternehmen Sinn. Externe Rechenzentren bieten deutlich mehr Sicherheit als ein eigener Serverraum. Solche Rechenzentren werden rund um die Uhr überwacht, haben ausgefeilte Zutrittssysteme und könnten selbst bei einem Stromausfall dank einer Notstromversorgung noch während mehreren Tagen weiterhin in Betrieb bleiben. Zudem bieten immer mehr Anbieter auch kleinste Einheiten zu bezahlbaren Preisen an; diese Rechenzentren sind also nicht mehr nur grossen Unternehmen vorbehalten.

Inwiefern spielen Cloud-Dienste bei der Auslagerung der Daten eine Rolle?

■ Die Cloud, also der Zugriff auf Rechner, die über das Internet erreichbar sind, gewinnt mehr und mehr an Bedeutung. Neu lassen sich ganze IT-Umgebungen in der Cloud realisieren. Server werden also nicht mehr selber angeschafft und im eigenen Serverraum betrieben, sondern nach Bedarf gemietet. Immer mehr Anbieter, so auch green.ch, bieten reine Schweizer Cloud-Lösungen an. Damit werden auch die hiesigen Datenschutzbestimmungen erfüllt.

Die Cloud schürt bei KMU auch Unbehagen, gilt gar als unsicherer Ort irgendwo im Nirgendwo.

■ Das ist eine häufige Aussage, wenn KMU zur Nutzung von Cloud-Diensten befragt werden. Tatsächlich lagern aber schon sehr viele Daten in Clouds, vom privaten Ferienfoto bis zum Geschäfts-E-Mail. Cloud-Dienste zeichnen sich durch ihre Einfachheit aus. Daten werden abgelegt und können von jedem Standort aus abgerufen werden. Um die Systeme hinter der Anwendung brauche ich mich nicht zu kümmern.

Wie schätzen Sie die Sensibilisierung für IT-Themen in der Schweizer Politik ein?

■ Im Parlament befassen sich rund 15 Politiker intensiv mit digitalen Themen, wir sind also ein sehr kleiner IT-affiner Politikerkreis. Dementsprechend stiefmütterlich werden diese Themen auch behandelt. Wir sehen uns mit immer mehr Bürokratie und Regulierung konfrontiert und teilweise technisch unsinnigen Massnahmen, wie etwa den Netzsperrern, die kürzlich beschlossen wurden. Doch gerade durch die fortschreitende Digitalisierung hätten wir die Chance, unser Land entscheidend weiterzuentwickeln – wenn wir jetzt die Weichen richtig stellen.

Interview: Gerhard Enggist

LINK

[www.green.ch](http://www.green.ch)