

# Sicher im Netz

Bei der Präsentation des Buches „Sicher im Netz“, im Amtsgebäude Rossau Bernardis-Schmid des Bundesheers, wurde betont, dass jeder seinen Teil zur Cyber-Sicherheit beitragen sollte.

Jeder hat in der vernetzten Welt eine Schlüsselrolle für die Cyber-Sicherheit“, sagte Mag. Klaudia Tanner, Bundesministerin für Landesverteidigung, anlässlich der Präsentation des Buches „Sicher im Netz“, am 28. September 2020 im Festsaal des Amtsgebäudes Rossau Bernardis-Schmid in Wien. „Jeder, betonte sie, müsse sensibilisiert sein und im Internet vorsichtig agieren. Die Bundesministerin erinnerte an den Angriff auf

die IT-Systeme des österreichischen Außenministeriums zu Jahresbeginn. Buchautor Oberst des Generalstabsdienstes Mag. Walter Unger erklärte die Details des Cyber-Angriffs: Lokalen Hilfskräften einiger Botschaften wurde eine E-Mail mit Weihnachtsgrüßen vom Ministerium in Wien geschickt, mit einem Anhang, der auf eine YouTube-Datei verwies. Das Raffinierte daran war, dass diese Grußbotschaft einer im Vorjahr versendeten täuschend ähnlich nachgebildet war. Eine Handvoll Empfänger der Mail haben den Link zur Datei angeklickt und dadurch einem Schadprogramm den Weg eröffnet, über den an Staatsgeheimnisse heranzukommen versucht wurde.

Im Zusammenwirken mit dem Innenministerium konnte das Datenleck geschlossen und der Angriff abgewehrt werden. Einem ähnlichen Angriff war auch der Telekommunikationsanbieter A1 ausgesetzt, mit dem Ziel, an vertrauliche personenbezogene Daten heranzukommen.

**Die Landesverteidigung** erstreckt sich auch auf den Cyber-Raum, was die Ministerin insofern als große Herausforderung bezeichnete, als sich Cyber-Methoden und Cyber-Angriffe besonders gut für die Austragung von Konflikten eignen würden. Das Bundesministerium für Landesverteidigung (BM-LV) werde in diesen Bereich der Abwehr investieren und die schon vorhandene gute Basis ausbauen. Eine anspruchsvolle Aufgabe dabei sei, die



Präsentation des Buches „Sicher im Netz“: Walter Unger, Klaudia Tanner, Manfred Lappe.

hierfür erforderlichen Spezialisten zu gewinnen, sagte die Verteidigungsministerin.

**Beispiele.** Im Buch „So schützen Sie sich vor Hackern und Betrügern“ (es wird in dieser Ausgabe bei den Buchrezensionen besprochen), finden sich zahlreiche Beispiele, wie man über das Internet zu Schaden kommen kann, und wie man sich davor schützt. Die beiden Autoren, Oberst Mag. Walter Unger, Leiter der Abteilung Cyber-Verteidigung im Abwehramt des Bundesheeres, sowie Diplomkaufmann Manfred Lappe, schilderten bei der Präsentation selbst Erlebtes, wie etwa, dass die zehnjährige Tochter über Internet einen Abo-Vertrag abgeschlossen hatte, oder die 84-jährige Mutter einem angeblichen IT-Techniker am Telefon arglos ihr Passwort mitgeteilt hatte. Die meisten der im Buch geschilderten Angriffe würden, so meint man als Leser, erfolglos bleiben, wenn man mit gesundem Hausverstand an Versprechungen und Verlockungen herangehen würde.

**Herr Oberst, haben Sie eine Erklärung dafür, warum viele Internet-Betrügereien wohl keinen Erfolg gehabt hätten, wenn man ein wenig Vorsicht hätte walten lassen?** Ich sehe das Problem darin, dass in den letzten zwei Jahrzehnten eine Technologie entstanden ist, mit der die Elterngeneration nicht Schritt gehalten hat. Von den Eltern lernen die Kinder Verhaltensweisen, lernen Schwimmen, Rad- und

Schifahren und werden auf Gefahren in Alltagssituationen hingewiesen. In der Internetnutzung mit all den Bildern und Möglichkeiten werden die Kinder – abgesehen von Verboten, die nicht verstanden werden – allein gelassen. Und ähnlich allein gelassen ergeht es den Eltern, wenn sie sich nicht selbst um tieferes Verständnis bemühen. Zu sehr wird auf die Technologie vertraut oder werden auch simple technische Vorsichtsmaß-

nahmen außer Acht gelassen. Private Initiativen, wie etwa die von der Frau Ministerin erwähnte Initiative fit4internet, sind wichtig, digitale Kompetenz in die Bevölkerung zu bringen.

**Auf den verschiedensten Ebenen finden doch Schulungen im IT-Bereich statt. Wie beurteilen Sie deren Nutzen?**

Schulungen im IT-Bereich müssen in Anbetracht der raschen Entwicklung vor allem regelmäßig und kontinuierlich erfolgen. Im Grunde genommen ist es eine Sisyphus-Arbeit. Menschen, die eine Einschulung erhalten haben, wechseln auf andere Posten, neue rücken nach – man muss wieder von vorne anfangen. Aber das muss man auf sich nehmen, bis sich ein gewisser Grundstock an Wissen herausgebildet hat.

**Das Internet-of-Things bringt den direkt mit dem Internet verbundenen Kühlschrank, die Waschmaschine, den Fernseher. Was ist, wenn diese Geräte gehackt werden, Schadfunktionen entfalten oder beispielsweise Teile von Botnetzen werden?**

Die Industrie müsste dazu gebracht werden, von billigen Chips abzugehen und sichere elektronische Bauteile, etwa mit 2-Faktor-Authentifizierung, einzubauen. Es könnte ein digitales Gütesiegel entwickelt werden, zusammen mit Haftungsansprüchen gegenüber dem Hersteller, wenn die für IT-Produkte zu fordernden Qualitätsansprüche nicht eingehalten werden und dadurch Schaden entsteht. *Kurt Hickisch*