Vorstellung der „Cyber Security Challenge“: Christian Kunstmann (KSÖ) und Joe Pichlmayr (CSA).

„Cyber Security Challenge“: Die talentiertesten Jung-Hacker des Landes sollen ermittelt und beruflich gefördert werden.

Ganzheitliches Denken

In ersten Jahr seines Bestehens hat der Verein „Cyber Security Austria“ bereits eine Reihe von Aktivitäten zur Erhöhung der IKT-Sicherheit gesetzt – weitere folgen.

Die Statuten des am 18. Mai 2011 gegründeten Vereins „Cyber Security Austria – Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur“ mit dem Sitz in Wien sehen vor, die Kompetenzen von unterschiedlichen Informationssicherheitsbereichen zu erfassen, vernetzen, vermitteln und zu publizieren sowie das Sicherheitsbewusstseins in Österreich zu fördern.

Es soll aufgezeigt werden, wie sehr die Informations- und Kommunikationstechnik (IKT) bereits alle Lebensbereiche durchdrungen hat – und was passiert, wenn diese Technologie ausfallen sollte, erläutert der Obmann und Sprecher des Vereins, Paul Karrer. „Vernetztes Denken ist notwendig. Wenn beispielsweise Katastrophenschutzübungen unter der Annahme durchgeführt werden, dass die Kommunikationsmittel wie gewohnt funktionieren und dass elektrische Energie zur Verfügung steht, werden wesentliche Faktoren nicht berücksichtigt.“ Es geht um Bewusstseinsbildung, dass es eben nicht selbstverständlich ist, dass der Strom aus der Steckdose kommt, dass Wasser aus der Leitung fließt, wenn der Wasserhahn aufgedreht wird, und dass man jederzeit mit jedem in Kontakt treten kann. Hinter all dem stecken hochkomplexe, auf Informationstechnologie beruhende Steuerungssysteme, die ausfallen oder gezielt gestört werden können.

CSA ist ein Zusammenschluss von ehrenamtlich tätigen Privatpersonen, die ihr Fachwissen einbringen.

Safety/Security. Der Schwerpunkt des heutigen Sicherheitsdenkens liegt auf dem Gebiet der Safety, der technischen Sicherheit von Maschinen und Geräten. Gesetze, Normen schreiben bis ins Detail vor, welche Sicherheitsmaßnahmen am Arbeitsplatz und zum Schutz der Umwelt zu ergreifen sind, wie Maschinen sicher gemacht werden können.

Interessensvertretungen kümmern sich um die Einhaltung dieser Bestimmungen und fördern die Weiterentwicklung. Wer aber kümmert sich darum, dass beispielsweise die Steuerungsanlagen von Maschinen und Anlagen nicht manipuliert werden können? Wer bedenkt die innere Sicherheit von Systemen – die Security? Nicht einmal ein Kühlschrank oder eine Waschmaschine kommen heutzutage ohne Chip und damit Informationstechnologie aus, gibt Karrer zu bedenken. Noch viel weniger ist das der Fall bei im industriellen Arbeitsprozess eingesetzten, von Programmen und über das Internet gesteuerten Maschinen, bis hin zu Basisbereichen des modernen Lebens, etwa der Energieversorgung.

Mit dem Zugang zur Fernwartung von Anlagen wird oftmals fahrlässig umgegangen. Passwörter werden nach der Installation nicht geändert, das erleichtert Angriffe etwa auf Heizungsanlagen oder Kühlhäuser.

Bei Unternehmen müssen Risiken, wie sie durch den Ausfall der IKT eintreten können, erfasst und finanziell bewertet werden. Auch dazu will der Verein Aufklärungsarbeit leisten.

Hacker Challenge. „Wir haben ungenütztes Potenzial in der technikbegeisterten Jugend. Allen jenen, die als Hacker in fremde Informationssysteme eindringen, um sich und Gleichgesinnten dadurch ihre Fähigkeiten zu beweisen und in der Community einen Namen zu machen, wollen wir ein Betätigungsfeld bieten“, führte Karrer aus.

Mit dem *Kuratorium Sicheres Österreich* wurde am 28. Juni 2012, im Rahmen des Sicherheitskongresses in Wien, die „Cyber Security Challenge Austria 2012“ gestartet und das Hacking-Lab freigeschaltet. Anmeldungen sind unter *www.verbotengut.at* möglich.

Ziel ist es, den 14- bis 15-Jährigen die Möglichkeiten zu bieten, ihre Fähigkeiten beim Eindringen in IKT-Systeme in einem fairen Wettstreit zu messen. Nicht der akademische Nachwuchs, dem andere Möglichkeiten zur Verfügung stehen, soll angesprochen werden, sondern Jugendliche, die oftmals ein erstaunliches Fachwissen besitzen. „Das sind die künftigen IT-Sicherheits-

Fotos: BMI, Egon Weissheimer

Kritische Infrastruktur: Mit dem Zugang zur Fernwartung von Anlagen wird oftmals fahrlässig umgegangen.

leute, die die Wirtschaft brauchte“, betont Karrer. Die Teilnehmer arbeiten in einem geschlossenen System. Die Aufgaben werden in den Schwierigkeitsgraden leicht, mittel und schwer gestellt. Mit Stand Mitte Juli haben sich bereits über 200 Teilnehmer angemeldet. Zwölf davon haben bereits sehr schwere Aufgaben gelöst.

In der ersten Vorrunde werden von Juli bis Oktober jeden Monat Aufgaben ins Netz gestellt und von Coaches bewertet. Es besteht die Möglichkeit, die Lösungen zu begründen und mit dem Coach zu diskutieren.

In der zweiten Finalrunde werden die zehn besten Teilnehmer aus der Vorrunde in zwei Teams eingeteilt, die in einer Live-Challenge gegeneinander antreten. Das Finale wird am 6. und 7. November 2012 im Burgenland beim 10. IKT Sicherheitskongress des Verteidigungsministeriums ausgetragen. Die Siegerehrung samt Preisverleihung findet am 8. November 2012 im Heeresgeschichtlichen Museum in Wien statt.

Arbeitsgruppen. Der Verein hat verschiedene Arbeitsgruppen eingerichtet. Zum Thema Smart Metering wurde das Schluss-Dokument nach eineinhalbjähriger Arbeit fertiggestellt; es wird auf der Website des Vereins publiziert.

Ein weiteres Arbeitsthema sind die „Smart Grids“, da nach der Hoch- und Mittelspannungs-Ebene nun auch die Niederspannungsebene der elektrischen Energieversorgung automatisiert wird. Damit einhergehende Risken sollen erforscht und es soll nach Abhilfen gesucht werden.

In rechtlicher Prüfung befindet sich derzeit ein Projekt, das zu einem sorgfältigeren Umgang mit Kopierern führen soll. Moderne Kopiergeräte speichern die erstellten Kopien auf Festplatte. Die Geräte und damit auch das Speichermedium sind, zur Fernwartung, an das Internet angeschlossen, in vielen Fällen ohne ausreichenden Schutz vor Zugriffen auf die gespeicherten Daten.

Über den eigenen Kopierer könnte den Betreibern der Geräte in Form von Ausdrucken Mitteilungen zugesendet werden, dass ihr System Angreifern offensteht, und es könnten ihnen Sicherheitshinweise übermittelt werden. Der Verein arbeitet des Weiteren auch bei der Entwicklung der nationalen Sicherheitsstrategie mit (*www.digitales.oesterreich.gv.at*).

Kurt Hickisch

www.cybersecurityaustria.at

FOTO: EGON WEISSHEIMER