Wo viel Licht, da viel Schatten

(BS) Arne Schönbohm, BSS BuCET Shared Services AG, verdeutlichte in Bad Neuenahr-Ahrweiler die Möglichkeiten, aber auch die Verwundbarkeit der vernetzten Wissensgesellschaft des 21. Jahrhunderts. "Cloud Computing, Milliarden von Apps auf Smartphones, Smart Grids. Alles wird über die Vernetzung effizienter, in großen Teilen auch kostengünstiger. Aber all das basiert auch auf dem Internet. Verknüpfung führt zu Effizienz und zu Verwundbarkeit gleichzeitig", so Schönbohm.

Die Cyber-Kriminalität sei, dies zeigten Statistiken und Analysen, heute wirtschaftlich gesehen gewinnbringender als etwa die Drogenkriminalität. Und genau dies sei auch ein wichtiges Thema für die Kommunen. Dies verdeutlichte Schönbohm an verschiedenen Beispielen der zunhemenden Cyber-Kriminalität. Dazu zählten etwa ein Datenhack in Österreich, bei dem 25.000 Daten, Namen und Privatadressen von Polizisten gehackt wurden. Andere Beispiele sind das Einhacken in die Steuerungskontrolle eines Reisezuges in den Vereinigten Staaten oder auch Cyber-Angriffe auf Krankenhäuser. "Daten und Informationen sind das Öl des 21. Jahrhunderts. Sie als Bürgermeister sitzen in Ihren Gemeinden auf Ölquellen", so Schönbohm. Jede Kommune habe sensible Daten, gleichzeitig in vielen Fällen aber auch eine gewisse Unsensibilität gegenüber Passwörtern, die allzu gerne auf den Rückseiten der Laptops stehen.

Arne Schönbohm betonte in Bad Neuenahr-Ahrweiler die Vor- und Nachteile der vernetzten Gesellschaft.
Fotos: BS/Wagner

"Cyber-Angriffe auf Ihr Öl, auf die Daten und Informationen von Kommunen, sind nur noch eine Frage der Zeit. Eine weitere Frage ist, wie diese Angriffe dann ausgeführt werden und wie sie aussehen", betonte Schönbohm und unterstrich damit, dass gerade in den Kommunen ein dringender Handlungsbedarf bestehe.

Praxisorientierte Kompromisse notwendig

(BS) Das ein gezielter Schutz gegen Cyber Crime zwingend notwendig ist, verdeutlichte Prof. Dr. Peter Martini, Institutsleiter Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) zunächst anhand einiger Zahlen.

"2009 sorgte der Computer-Wurm Conficker für mediale Präsenz. Darüber wurden 2009 rund sechs Millionen Systeme infiziert. Im vergangenen Jahr wurden darüber aber immer noch rund drei Millionen Systeme infiziert", so Prof. Martini. Das Außmaß der Cyber Crime sei aber noch viel größer. Es seien derzeit rund 1.600 Command and Control Server von Botnetzen bekannt, die auch täglich Commands senden. Wie ein solcher Angriff über Botnetze aussieht, verdeutlichte Prof. Martini über das Beispiel von DDoS-Attacken: "Diese funktionieren letztendlich mit einer Intensität von 100 Gigabite pro Sekunde. Da hat niemand eine Chance".

An dieser Stelle setze dann die Organisierte Kriminalität (OK) ein. "Es geht um Erpressung, um etwa die Server eines großen Immobilienunternehmens am Laufen zu erhalten", so Prof. Martini weiter.

Prof. Dr. Peter Martini verdeutlichte, dass man bei Cyber-Angriffen schnell an verschiedene Grenzen stoße.

Eine passive Verteidiung gegen Cyber Crime reiche grundsätzlich nicht aus. Es müsste ein Problembewusstsein geschaffen werden. Vor allem aber müssten zwingend notwendige Ressourcen identifiziert und entsprechend gesondert geschützt werden.

Die Lösungsdomäne gegen Cyber-Angriffe bestehe aus drei Ebenen: Politik und Gesellschaft, Technologie sowie Prozesse and Policies. Hier seien Grenzen deutlich, zum einen in einem notwendigen Kompromiss zwischen Usability und Security, zum anderen stoße man im Kampf gegen Cyber-Angriffe aber auch schnell an rechtliche Grenzen. Hier müsse daher drimgend ein Umdenken stattfinden.