

## ++++ PRESSEMITTEILUNG +++++

LEIPZIG, 08.01.2019

### **Zwischen Spaß und Verbrechen – Cybercrime als gesellschaftliches Phänomen und existenzielles Risiko**

Festnahme eines Tatverdächtigen im Fall des Datenklaus im Bundestag zeigt Tragweite von Internetkriminalität / Cluster IT warnt vor breitgefächertem Gefahrenpotenzial

Er ist 20 Jahre alt, Schüler und wohnt noch bei seinen Eltern. So sieht das Profil des Tatverdächtigen aus Mittelhessen aus, der hunderte Datensätze von Politikern und Prominenten gestohlen und über Twitter veröffentlicht haben soll. Ein politisches oder wirtschaftliches Motiv ist nach Aussagen der Ermittler auf den ersten Blick nicht erkennbar. Über die Tragweite seiner Taten war sich der junge Mann nach bisherigem Stand selbst nicht im Klaren. Aus Sicht des Clusters IT Mitteldeutschland e. V. steht der Fall sehr deutlich für einen allgemeinen Trend: Gefahren durch Cybercrime drohen auf den unterschiedlichsten Ebenen – und machen das Problem so bedeutsam.

Gerd Neudert, Geschäftsführer Cluster IT Mitteldeutschland e. V.: „Wenn es um Internetkriminalität geht, rücken schnell ausländische Geheimdienste und terroristische Organisationen als Drahtzieher ins Visier. Tatsächlich besteht durch professionell angelegte Hackerangriffe, zum Beispiel in Form von Wirtschaftsspionage, ein großes Gefahrenpotenzial für Unternehmen, Organisationen und Menschen. Nicht selten drohen den Opfern dieser Cyberverbrechen existenzielle Schäden. Dennoch ist Internetkriminalität bei Weitem nicht nur auf professionelle, wirtschaftlich oder politisch motivierte Täter zurückzuführen. Das kürzlich erfolgte Beispiel, bei dem hunderte Daten von Politikern und Prominenten entwendet und über Twitter veröffentlicht worden, zeigt es deutlich: Der mutmaßliche Täter weist ein eher unauffälliges Profil ohne auf den ersten Blick erkennbare tiefgründige Absichten auf. Genau diesen Trend beobachten wir als IT-Branchennetzwerk schon seit Längerem. Internetkriminalität stellt zunehmend ein breites gesellschaftliches Phänomen dar, in dem die Angreifer aus den unterschiedlichsten Bereichen kommen und die vielfältigsten Motive haben. Auch diejenigen, die Hacking sozusagen ‚freizeitmäßig‘ betreiben, sind in diesem Zusammenhang nicht zu vernachlässigen. Zwar mögen diese Angriffe harmlos wirken, doch ihre Folgen können für die Betroffenen durchaus ernsthaft und gravierend sein.“

Sportlicher Ehrgeiz, Austesten von Grenzen und Machbaren sind einige Motive für privat betriebenes Hacking. Zum Teil stecken sogar ethische Motive hinter dem Handeln: Das gezielte Aufdecken von Sicherheitslücken soll auf Missstände hinweisen; die Veröffentlichung von bisher verborgenen Informationen für die Verbreitung von Wahrheit sorgen. So richtete der Chaos Computer Club nach Weihnachten seinen 35. Kongress in Leipzig aus. Das weltgrößte Treffen von Hackern mit rund 16.000 Teilnehmern widmete sich dabei zentral dem Thema Weltoffenheit und Faktentreue.

Was Internetkriminalität begünstigt, ist, dass teilweise allein ein gutes technisches Wissen erforderlich ist, um digitale Sicherheitslücken aufzudecken und auszunutzen. Dies liegt wiederum an den oftmals geringen oder gar nicht vorhandenen Abwehrmechanismen gegen Cybercrime. „Je ernster IT-Sicherheit genommen wird und je professioneller und umfangreicher man Schutzvorkehrungen gegen Cyberangriffe trifft, desto besser lassen sich die eigenen Daten gegen Diebstahl oder Missbrauch schützen“, so Neudert, „Dafür braucht es eine gut eingerichtete, moderne Technologie und die entsprechende Expertise. Gleichzeitig muss die Sensibilität für menschliche oder organisatorische Schwächen wachsen, die Lücken im Sicherheitsnetz begünstigen – wie das prominente Beispiel von extrem unsicheren Passwörtern.“

Der Cluster IT Mitteldeutschland veranstaltet zu diesem Zweck regelmäßig Events über Cybercrime, die auf die Gefahrenlage aufmerksam machen und Lösungsmöglichkeiten aufzeigen. Im Dezember fand eine Veranstaltung in dem Kontext in Leipzig statt. Weitere Events werden mitteldeutschlandweit ab Frühjahr 2019 folgen. Internetkriminalität ist außerdem Schwerpunkt des Arbeitskreises IT-Sicherheit im Cluster IT Mitteldeutschland. Experten aus führenden IT-Unternehmen widmen sich darin der Entwicklung und Etablierung von Schutzmechanismen gegen Cybercrime.

#### **Zum Cluster IT Mitteldeutschland e. V.**

Der Cluster IT ist das Branchennetzwerk der IT-Wirtschaft in Sachsen, Sachsen-Anhalt und Thüringen mit der Zielsetzung, die Aktivitäten der Branche zu koordinieren und sichtbar zu machen. Gegründet wurde der Verein im Jahr 2009 und besitzt mittlerweile knapp 50 Mitglieder. [www.it-mitteldeutschland.de](http://www.it-mitteldeutschland.de).