Oberstleutnant d.R. Dipl.-Ing. Günter Holzhauser

Digitale Sozialisation

Der Brandbeschleuniger für die Bedrohungen und Risiken der Zukunft

In unserer Informationsreihe über Cyber-Security besonders im industriellen Bereich schreibt der Autor zu diesem Thema in unregelmäßigen Abständen seine Beiträge. In dieser Ausgabe geht es um die sozialen Dienste, die privat und vermehrt zunehmend auch in der Industrie genutzt werden und dem „Datenklau" Tür und Tor öffnen. Günter Holzhauser ist Sektionsleiter Rhein-Main der Deutschen Gesellschaft für Wehrtechnik und Geschäftsführer der BUSINESS INTELLIGENCE & SECURITY in Eschborn.

Lassen sich die wirtschaftlichen Visionen mit der Sicherheit in Einklang bringen?

Fremde Nachrichtendienste, global agierende Unternehmen und zunehmend die organisierte Kriminalität (OK) beschaffen sich das Know-how und Informationen zur Entwicklung ihrer eigenen Märkte und kriminellen Geschäftsmodelle in Deutschland. Deutschland ist stark zunehmend Aktionsraum für das internationale Verbrechen. Seit jeher gehört Deutschland zu den bevorzugten Angriffszielen fremder und professioneller Angreifer. Die Grenzen zwischen Wirtschaftsspionage, CyberCrime und dem organisierten Verbrechen verschwimmen immer mehr. Nicht zu vergessen die stark wachsende und nichtlineare Bedrohung für Gesellschaft und Infrastruktur durch die vielfältigen Formen des Terrorismus und Extremismus.

Die stark zunehmende Globalisierung und Vernetzung unserer Welt wird durch die rasante Entwicklung von neuen Technologien getrieben. Die ständig fortschreitende digitale Sozialisation – unserer Gesellschaft und unserer Wirtschaft – bildet den Nährboden für das rasch zunehmende transnationale Verbrechen.

Die Bundesregierung und die Wirtschaft erhöhen das Tempo im Kontext der digitalen Sozialisation. Auf dem letzten Weltwirtschaftsforum in Davos hat die Bundesregierung der Industrie entsprechende Vorgaben ins Lastenheft geschrieben. Es soll sichergestellt werden, dass Deutschland im globalen Geschehen den Anschluss nicht verliert.

Die Metatrends im digitalen Zeitalter – Der Brandbeschleuniger für die Bedrohungen der Zukunft

Was sind die aktuellen neuen Entwicklungen und die Themen der Zukunft? Z.B. Social Media, mobile Endgeräte, vernetzte Mobilität, Internet der Dinge, Industrie 4.0 und Social Enterprise. Die Vernetzung von Mensch, Gesellschaft und Unternehmen schreitet unaufhörlich und mit rasantem Tempo voran. Alle Trends überlagern sich, sie vernetzen sich und stehen in Abhängigkeit zueinander. Hier entstehen komplexe und heterogene Netzwerke aus Menschen und Dingen mit Bedrohungen und Risiken, die wir heute noch nicht absehen können.

Verschiedene Experten gehen davon aus, dass in der Zukunft die Milliarden von mobilen Endgeräten noch unsicherer werden. Diese Anzahl von Geräten verteilt sich auf wenige unterschiedliche Betriebssysteme der Markführer. Weltweit arbeiten jetzt schon viele Millionen professionelle Angreifer mit unterschiedlichsten Motiven an Angriffswerkzeugen für Geräte und Menschen. Die Anzahl der Angreifer in der Zukunft wird dramatisch zunehmen, die digitale Sozialisation wird das Verbrechen leichter machen. Die deutschen Sicherheitsbehörden sprechen jetzt schon von einer massiven Zunahme der Angriffe in Qualität und Quantität.

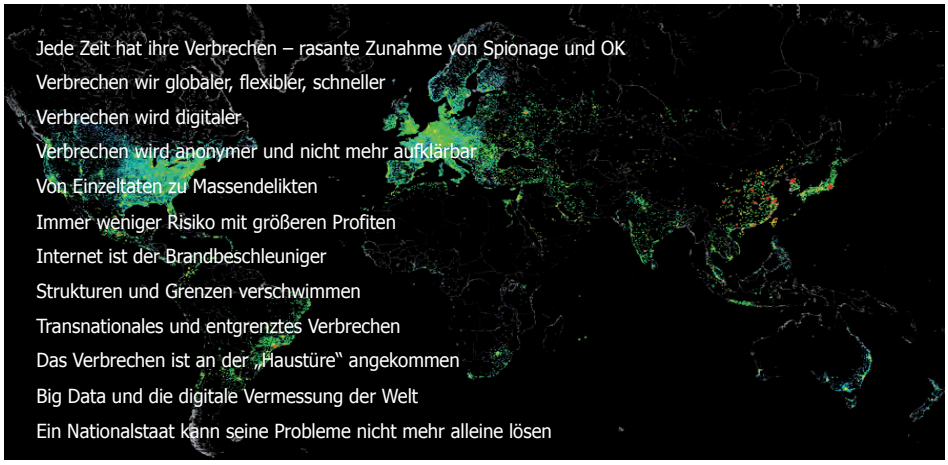
Die Anzahl der potenziellen Angriffsziele auf Menschen und Netzwerke steigt exponentiell. Die Beratungsfirma Gartner geht davon aus, dass im Jahre 2020 ca. 220 Milliarden Geräte mit dem Internet verbunden sein werden. Entstehen hier nicht Milliarden von potenziellen Sicherheitsrisiken in

SOZIALE NETZE DURCHDRINGEN UNSERE PRIVATE, ABER AUCH DIE GEWERBLICHE DATENWELT

Grafik: viking

Grafik: Autor

Lagebild transnationales Verbrechen



Form der Geräte und sogar der Menschen, die sich mit ihren Geräten in den Netzwerken bewegen?

Die Netzwerke der Zukunft können wir uns wie ein Spinnennetz vorstellen. Zieht man an einem Ende des Spinnennetzes (der erfolgreiche Angriff), dann hat dies Einfluss auf das ganze Gewebe und das Netz, es kommt in Bewegung. Unsere Netzwerke der Zukunft mit den vielen vernetzten und verbundenen Einzelakteuren bieten insgesamt eine enorme Angriffsfläche.

Bereits jetzt ist schon abzusehen, dass diese Trends und Entwicklungen dazu führen, zukünftig Menschen und vertrauliche Informationen schneller zu enttarnen, Menschen, Informationen und Prozesse schneller zu manipulieren und Produktionsnetzwerke/kritische Infrastrukturen schneller zu sabotieren. Aus meiner Sicht wird die Sabotage und die Desinformation in Zukunft eine der Hauptbedrohungen werden. Fremde Nachrichtendienste – damit Nationalstaaten – können sicherlich heute schon Netzwerke (z.B. Industrie 4.0) und kritische Infrastrukturen in verschiedenen Ländern per Mausklick manipulieren oder abschalten.

Gerade im Kontext von Industrie 4.0 verschwinden die territorialen Grenzen. Die klassischen hierarchischen Organisationen von Unternehmen werden sukzessive durch autonome und virtuelle Organisationen ersetzt. Im Vordergrund dieser Bestrebungen steht die Erhöhung der Produktivität durch Vernetzung und Sichtbarmachung von Menschen und Wissen.

Wenn wir angegriffen werden, stellt sich die Frage, sind wir die Opfer und die Unschuldigen oder sind wir durch unser Denken und Handeln selber Teil des Problems? Ich bin der Meinung, dass die komplexe und heterogene Bedrohungslage mit ihren noch nicht abzusehenden Risiken für die Metatrends Industrie 4.0, Internet der Dinge, vernetzte Mobilität und Social Business als Bedrohung in Politik und Wirtschaft noch nicht richtig angekommen ist.

Im Kontext von Bedrohungen und Risiken kann z.B. Industrie 4.0 nicht alleine gesehen werden. Im Kontext der Sicherheit müssen zukünftig die Netzwerke mit allen Beteiligten betrachtet werden, die Betrachtung einzelner Beteiligter oder Unternehmen greift zu kurz. Nur durch Bedrohungs- und Risikoanalyse eines Netzwerkes mit seinem Umfeld können notwendige Sicherheitsstrukturen abgeleitet werden. 100%ige Sicherheit gibt es heute nicht und wird es erst recht in Zukunft nicht geben.

Im Kontext der Sicherheit können diese Entwicklungen für Gesellschaft, Personen und die Wirtschaft verheerende Folgen haben, wenn für diese Entwicklungen die Sicherheitsarchitektur vernachlässigt wird. Fremde Geheimdienste und Angreifer freuen sich sicherlich über diese Entwicklung. Mit den bereits heute vorhandenen Technologien der Nachrichtendienste eröffnet sich ein breites Spektrum für Angriffe.

Was kann in Bezug auf die Wirtschaft getan werden?

Wir sollten uns bewusst werden, dass wir in Deutschland an der Spitze der auszuspähenden und angegriffenen Länder liegen.

Verbrechen ist unabhängig von Unternehmensgröße, Branche und Wertschöpfungstiefe. Kleine mittelständische Unternehmen sind genau so betroffen wie große Konzerne. Der Verbund von Unternehmen und Organisationen zu Industrie 4.0 bietet sogar noch mehr Angriffsfläche als die einzelnen beteiligten Unternehmen. Das Thema Sicherheit im Kontext dieser Metatrends wird aus meiner Sicht in Deutschland massiv unterschätzt. Viele Unternehmen, die auf den Zug aufgesprungen sind, haben keine Transparenz über die Bedrohungen und Risiken, die im Kontext dieser Visionen existieren. Oftmals sind Risiko- und Bedrohungsanalysen oder Umfeldanalysen in vielen Unternehmen Fremdwörter. Die Problematik gilt sicherlich auch für Regierungsorganisationen, Behörden und die Hochschulen.

Die Nationale Wirtschaftsschutzstrategie der Bundesregierung ist der notwendige und richtige Schritt. In ihr erarbeiten aktuell verschiedene Arbeitsgruppen mit Beteiligten aus Regierung, Sicherheitsbehörden, Verbänden und der Wirtschaft Strategien zum Schutze unserer deutschen Wirtschaft.

Eines kann jedoch mit Sicherheit gesagt werden, dass wir die Bedrohungen und Risiken der Zukunft noch nicht abschätzen können. Bisher war die Sicherheitsarchitektur oftmals opportunistisch getrieben. Dies wird sich nicht ändern. Ich hoffe, dass der Vorsprung der Angreifer in Zukunft nicht noch größer wird. ■