Cyber-Angriffe gegen Estland - Lehren für Österreich

Zuerst erschienen in:
ÖMZ
ÖSTERREICHISCHE MILITÄRISCHE ZEITSCHRIFT
01 2009

Cyber-Angriffe gegen Estland - Lehren für Österreich

Walter J. Unger

Technologisch weist Estland eine weit fortgeschrittene Informations- und Kommunikationstechnikinfrastruktur (IKT) von Staat und Gesellschaft auf. Estland verfolgt seit Jahren die Strategie, die veralteten Infrastrukturen durch moderne Informations- und Kommunikationstechnologie zu ersetzen. Das konsequente Beschreiten dieses Weges führte Estland im e-Government-Ranking der EU im Jahr 2006 an die dritte Stelle: 107% Abdeckung mit Mobiltelefonie, 97% aller Bankgeschäfte laufen elektronisch ab, alle Schulen sind mit dem Internet vernetzt, e-Voting ist gelebte Realität. Dies legt ein beredtes Zeugnis vom Grad der Vernetzung Estlands ab.
Im April und Mai 2007 war Estland Ziel heftiger Cyber-Angriffe.

Auslöser der Angriffe

Am 27. April 2007 beschloss die estnische Regierung, das Denkmal des russischen Soldaten vom Hauptplatz auf einen Soldatenfriedhof am Stadtrand zu verlegen. Dies führte zur Eskalation der politischen Propaganda und zum Ausbruch von Unruhen, in deren Verlauf eine Person zu Tode kam und mehr als 100 Personen verletzt wurden. Gleichzeitig demonstrierte in Moskau die Jugend der regierenden Partei „Haus Russland “ vor der estnischen Botschaft. Im Internet wurde zu Angriffen auf estnische Internetseiten aufgerufen.

Verlauf der Cyber-Angriffe

Die Cyber-Angriffe[1)] rollten in drei Phasen ab: Phase 1 vom 27. bis 29. April, Phase 2 vom 30. April bis 18. Mai und die anschließende Folgephase seit 19. Mai.

Die erste Phase war geprägt von offensichtlich wenig vorbereiteten Attacken zum Zweck der Verunstaltung von Webseiten der Regierungs- und anderer estnischer Parteien. In der Folge zielten DoS- und DDoS-Angriffe,[2)] basierend auf mutmaßlich kleineren Bot-Netzen,[3)] gegen Regierungsseiten. Spam-Attacken[4)] legten E-Mail-Adressen von estnischen Regierungsvertretern lahm. Die Seiten der Nachrichtenagenturen gingen während der Angriffe offline und waren mehrere Tage nicht erreichbar.
Ab 30. April starteten koordinierte Angriffe, abgestützt auf größere Bot-Netze. In dieser Phase 2 konnten mehrere Angriffswellen beobachtet werden, von denen einige zeitweise erfolgreich die kritische Informationsinfrastruktur (Critical Information Infrastructure/CII) Estlands beeinträchtigten. Einige Attacken trafen die Router der Internet Service Provider (ISP). Durch Überfluten mit großen Datenmengen (Data Overflow) kam es zeitweilig zu Unterbrechungen von Teilen der Netzwerke. Kurzzeitig war sogar die Regierungskommunikation unterbrochen. Die raschen Reaktionen der Angreifer auf Abwehrmaßnahmen, - Anpassung und Verfeinerung der Angriffsmethoden -, lassen den Schluss zu, dass entsprechend qualifizierte, erfahrene und wissende Angreifer am Werk waren.
Heftige Attacken gegen Provider führten zeitweise zur Unterbrechung des DNS.[5)] DDoS-Angriffe (ping flood, syn flood, malformed GET queries) [6)] über Bot-Netze mit bis zu einer Million Zombies[7)] konnten festgestellt werden. Diese intensivsten Angriffe fanden am 4. bzw. vom 9. auf den 10. Mai statt, größere Angriffe gab es auch am 15. und 18. Mai. Zu diesem Zeitpunkt wurden durch Abwehrmaßnahmen (Filter an den Eintrittspunkten) Angriffe von rund vier bis fünf Millionen pps[8)] auf 7.000-8.000pps im Ziel gefiltert. Dennoch waren einige der attackierten Regierungsseiten erheblich beeinträchtigt. Am 10. und am 15. Mai waren die zwei größten Banken Estlands mit zusammen 85% Marktanteil Angriffsziele. Seit dem 19. Mai bis dato werden laufend kleinere Angriffe festgestellt.

Ursachen der Angriffe und Motivation der Angreifer

Die Cyber-Vorfälle müssen in einem weiteren Rahmen beurteilt werden. Dieser umfasst politische Stellungnahmen russischer Regierungsvertreter, anonyme Aufrufe zur physischen Gewalt, Angriffe gegen die estnische Botschaft in Moskau und versteckte Wirtschaftssanktionen gegen Estland. Die Ursachen sind in der exponierten Lage Estlands am Rande der EU sowie in der belasteten Geschichte zwischen den dort lebenden rund 921.000 Esten und den rund 345.000 Russen zu finden.
Aufgrund der Geschichte - die russische Minderheit fühlt sich als Befreier Estlands aus der nationalsozialistischen Unterdrückung, die Esten sehen in den Russen nach wie vor sowjetische Besatzer - stellt sich das Zusammenleben zwischen den beiden Ethnien als sehr schwierig dar. In den 1990er-Jahren wurde den estnischen Russen die Staatsbürgerschaft aberkannt und diese sind nunmehr staatenlos, wenn sie nicht nachweisen können, dass sie oder ihre Vorfahren schon vor dem Zweiten Weltkrieg in Estland gelebt haben.
Im Vorfeld wurde die russische Regierung durch den russischen Föderationsrat aufgefordert, „härtest mögliche Maßnahmen“ gegen Estland zu ergreifen. Eine Abordnung der russischen Duma verlangte schon vor einer Reise nach Tallinn den Rücktritt der estnischen Regierung. Weiters hat die russische Regierung Estland als faschistisch bezeichnet und der Geschichtsfälschung geziehen. Damit ist die ideologische Unterstützung der Cyber-Angriffe gegen Estland zumindest indirekt nachvollziehbar.
Auslösendes Motiv der Angriffe war der Beschluss zur Verbringung der Statue. Während der Cyber-Angriffe waren etliche Aufrufe zur Anwendung physischer Gewalt zu vernehmen. Eine „Armee des russischen Widerstandes Kolyvan“ zirkulierte in russischer Sprache in Internetforen. Darin wurden alle Russen in Estland aufgerufen, zu den Waffen zu greifen; ein Beispiel für einen terroristischen Zugang zu diesem Konflikt.

Vom 27. April an wurde die estnische Botschaft in Moskau von der Jugendbewegung der Kremlpartei Nashi[9)] gut organisiert belagert. Steine wurden auf die Botschaft geschleudert, die Hausmauern mit Farben verunstaltet, der Zugang blockiert und der estnische Botschafter bei einer Pressekonferenz am 2. Mai persönlich angegriffen - alles unter den Augen der nicht eingreifenden russischen Polizei.
Auch Wirtschaftssanktionen versteckter Natur konnten beobachtet werden: Eine Brücke von Russland nach Estland wurde für den Schwerverkehr gesperrt. Ab 3. Mai erfolgten Reparaturarbeiten an nach Estland führenden Bahnlinien, Öl- und Transithandel wurden dadurch unterbrochen. Am 3. Mai wurden alle Verträge der estnischen Firma Kalev mit Russland gekündigt.

Von estnischer Seite werden die Angriffe im Zusammenhang mit einem groß angelegten russischen Propagandafeldzug gesehen.[10)] Demnach seien russische Militärs schon seit längerem auf der Suche nach neuen Waffen und Konzepten zur Destabilisierung „einer Gesellschaft von innen“. Psychologische Operationen, elektronische Kampfführung und andere unkonventionelle Kampfformen seien konzeptiv bearbeitet worden. Es überrascht daher in Estland nicht, dass in diesem Konflikt so umfangreich mit Propaganda gearbeitet wurde. Während russische Politiker (in Russland und Estland) jede Möglichkeit nutzten, den Konflikt zu politisieren, wurden sie von russischen Medien und politischen Gruppen umfangreich unterstützt.
Die Verunstaltung russischer Webseiten am 9. Mai wird von estnischer Seite als Ablenkungsmanöver und mutmaßliches Werk russischer Hacker beurteilt, mit den Zielen, einerseits Spuren zu verwischen, andererseits sympathisierende Hacker zu Angriffen gegen Estland aufzurufen.

Bewertung der Angriffe

Die Cyber-Angriffe auf Estland müssen als Teil des allgemeinen politischen Konfliktes Estland-Russland gesehen werden. Die Cyber-Angriffe intensivierten die schon bestehenden Spannungen zwischen den beiden Ländern. Primäre Angriffsziele waren nicht die Websites von Behörden und Unternehmungen, sondern die nationale estnische kritische IKT-Infrastruktur.
Daraus ist die hohe sicherheitspolitische Bedeutung dieser Bedrohungsform erkennbar. Das Überdenken und Anpassen nationaler Verteidigungspolitiken ist zwingend geboten. Cyber-Angriffe stellen reale und aktuelle Bedrohungen für strategische, von der IKT abhängige Infrastrukturen dar. Krise, Spannungs-, Verteidigungsfall haben in diesem Zusammenhang eine völlig andere Bedeutung. Die nationale Zusammenarbeit von Regierung/Behörden mit der Wirtschaft, Wissenschaft und auf internationaler Ebene war ausschlaggebend für die Schadensbegrenzung und die rasche Wiederherstellung des ordnungsgemäßen Betriebes.
Die Angriffe blockierten zwar teilweise die Informationszugänge aus dem Ausland, beeinträchtigten das tägliche Leben aber kaum. Trotz enormem Netzwerkverkehr war die kritische Infrastruktur Estlands insgesamt wenig geschädigt, die Regierungsbehörden waren in geringem Ausmaß beeinträchtigt.
Estland ist ein Modell für einen Staat im Übergang in eine hoch entwickelte Informationsgesellschaft. Die zunehmende Abhängigkeit der strategischen Infrastrukturen vom Funktionieren der Informations- und Kommunikationstechnologie offenbart einige zu Angriffen einladende Schwachstellen. Zur Bewertung der Lehren aus den Angriffen für andere Staaten ist eine allgemeine Bedrohungsanalyse durchzuführen.

Bedrohungsanalyse

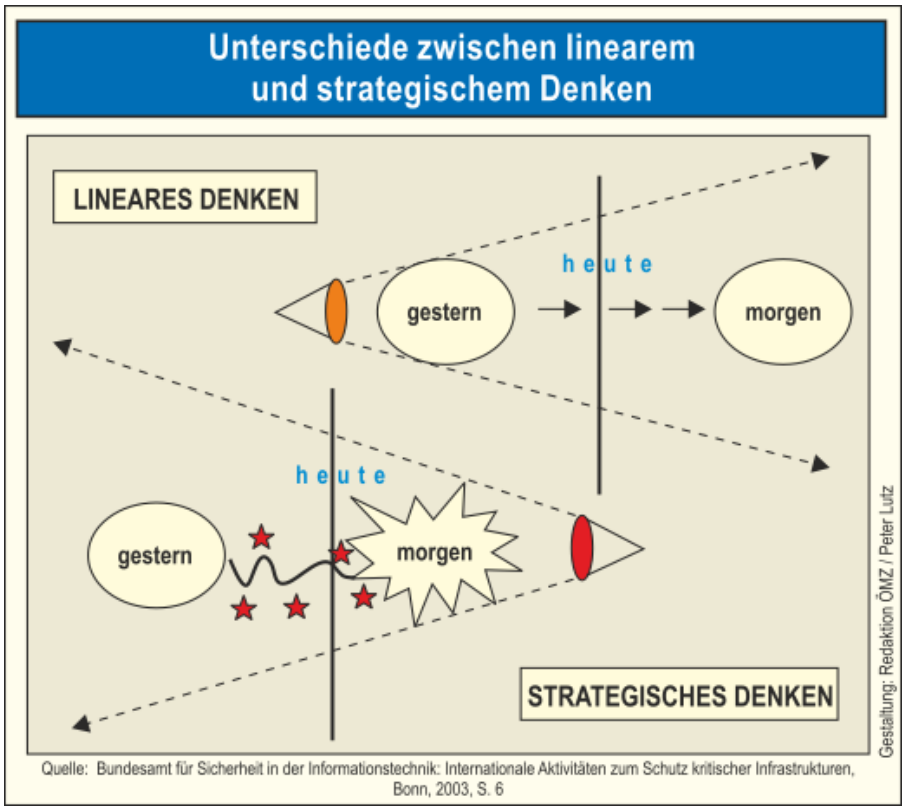
Mutmaßliche Angriffsziele bei einem Cyber-Angriff stellen die Grundwerte - Verfügbarkeit, Vertraulichkeit, Integrität - der kritischen, strategischen, auf IKT basierenden Infrastrukturen eines Staates dar. Ein Angriff auf nicht abgeschottete strategische IKT-Infrastrukturen kann aufgrund der weltweiten Vernetzung von jedem Punkt der Erde ausgehen. Die Nachvollziehbarkeit und Identifikation als eine von außen kommende Bedrohung[11)] wird dadurch erheblich erschwert. Selten wird es daher möglich sein, Angriffe auf die IKT konkreten politischen Akteuren oder gar Völkerrechtssubjekten klar zuzuordnen. Die geringen Kosten für die Durchführung eines Angriffes erweitern den potenziellen Täterkreis. Nicht nur Staaten, sondern auch Gruppierungen und sogar Einzeltäter kommen als Angreifer in Frage. Angriffe auf die IKT werden daher entweder als ein „bewaffneter Angriff" im Sinne des Artikels 51 der UNO-Charta oder als ein politischer oder allgemein „krimineller Akt" zu qualifizieren sein. Politische, ideologische, religiöse, ethnische, aber auch ökonomische, anarchistische oder persönliche Motivationen sind möglich. Insgesamt ist ein breites Spektrum von Angreifern, Tätern und deren Motivation vorstellbar.
Sogar Einzelpersonen könnten Angriffe auf IKT-Systeme aus persönlichen Motiven wie Bereicherung, Neugier, Verärgerung, Rache oder Erpressung durchführen.
Als Angriffsmittel und -methoden eignen sich das Einbringen von bösartiger, Schaden verursachender Software, die Einbringung von schadhafter Hardware ebenso wie die Anwendung von Methoden zur Sabotage, Störung bzw. Lähmung der IKT.
Die Vorteile für den Angreifer liegen in den preiswerten Mitteln, der geringen Entdeckungswahrscheinlichkeit sowie der Unabhängigkeit von Zeit und Ort. Die Vorbereitung eines Angriffes ist grundsätzlich schwer bzw. gar nicht erkennbar, daher wird die Vorwarnzeit für den Angegriffenen kurz bzw. nicht gegeben sein. Angriffsziele können in sehr kurzer Zeit erreicht werden, und in Hinblick auf eine allfällig beabsichtigte Folgenutzung könnte der Zerstörungsgrad beim Angegriffenen begrenzt werden.
Darüber hinaus können gleichzeitig herkömmliche Mittel und Methoden elektronischer sowie physischer Angriffe auf kritische IKT-Strukturen (z. B. Brandanschläge, Bomben, EMP, Mikrowellen- und Lasertechnologie) zur Anwendung kommen.
Das konkrete Ausmaß der allfällig verursachbaren Schäden kann nur nach einer Detailanalyse der potenziell gefährdeten IKT-Systeme eingeschätzt werden, da insbesondere der Vernetzungsgrad und die dadurch entstandenen Abhängigkeiten zwischen den strategischen IKT-Ressourcen nicht ausreichend bekannt sind. Bei der Analyse müssen Dominoeffekte und Kaskadenwirkungen sowie entstehende Sekundär- und Tertiärwirkungen/-schäden besonders berücksichtigt werden.
Neben den durch vorsätzliche Handlungen ausgehenden Bedrohungen sind katastrophale Schäden der strategischen IKT, verursacht durch höhere Gewalt oder technisches und menschliches Versagen zu berücksichtigen.
In Estland waren die Netze der Regierung, Behörden, politischen Parteien und Banken Ziel von zum Teil auch koordinierten Angriffen. Das Szenario eines Cyber War würde entstehen, wenn zusätzlich Angriffe auf die Energieversorgung, insbesondere der mit elektrischem Strom, auf die Zentralen der Telekommunikationsversorger, die Sicherheitsinstrumente für die innere und äußere Sicherheit, Polizei und Militär sowie auf Fernseh- und Radiostationen lanciert würden. Koordinierte Angriffe, allenfalls kombiniert mit herkömmlichen Methoden, wären geeignet, ein Land nicht nur für Stunden, sondern für lange Zeit lahm zu legen. Eingebettet in eine gesamtheitliche offensive Strategie könnten damit politische Ergebnisse erzwungen werden. Insbesondere Kleinstaaten müssen sich gegen diese potenzielle Bedrohung strategisch und operativ vorbeugend wappnen.
Ein Szenario in Anlehnung an die in Estland beobachteten Angriffe eignet sich einerseits zur Verbildlichung eines Krieges im Cyber Space. Andererseits bietet es eine Grundlage für strategische Ableitungen zur Abwehr derartiger Attacken.

Lehren für Österreich - Strategie zum Schutz des nationalen Cyber Space

Strategie soll Macht in Politik umsetzen,[12)] wobei die Natur der Machtfaktoren entsprechend zweitrangig ist. In fast übereinstimmender Sicht lässt sich Cyber War, eingebettet in einen „strategischen Informationskrieg", dem von Beaufre entwickelten Strategiebegriff zuordnen. Ziel jeder Strategie ist es demzufolge, die von der Politik gesetzten Aufgaben unter bestmöglicher Verwendung der verfügbaren Mittel zu erreichen.[13)] Die erstrebte Entscheidung im Kampf besteht darin, dass der Gegner die ihm auferlegten Bedingungen annimmt. In dieser Dialektik der Willen wird die Entscheidung zu einer psychologischen Reaktion, die man beim Gegner hervorrufen will: Er soll davon überzeugt sein, dass es nutzlos sei, den Kampf aufzunehmen oder fortzusetzen.[14)]
Wenn Cyber War das offensive strategische Konzept darstellt, müssen potenziell gefährdete Staaten - alle, die in einem erheblichen Ausmaß vom Funktionieren ihrer kritischen, auf Informations- und Kommunikationstechnik basierenden Infrastruktur abhängig sind - strategische Schutzkonzepte entwickeln und implementieren.

Strategische Vision

Strategisches Denken[15)] zeichnet sich durch die visionäre Verknüpfung der Gegenwart mit einer als wünschbar analysierten Zukunft aus. Dabei ist zunächst die Vision der Zukunft darzustellen. Denkbare, über die heutigen Leistungsfähigkeiten hinausgehende Möglichkeiten sind zu beschreiben. Ohne Vision besteht die Gefahr der Fortschreibung der Gegenwart in die Zukunft und der Verzettelung in Einzelmaßnahmen.
Strategisches Denken verlangt zunächst die Beantwortung der Fragen nach dem „Morgen": Was sind morgen Ziel und Zweck? Wie sieht morgen das strategische Umfeld aus? Im Sinne einer Rückwärtsplanung werden der Weg in die Zukunft und die Etappenziele bis in die Gegenwart zurückverfolgt.
Unterschiede zwischen linearem und strategischem Denken[16)].



Quelle: Bundesamt für Sicherheit in der Informationstechnik: Internationale Aktivitäten zum Schutz kritischer Infrastrukturen, Bonn, 2003, S. 6

Eine wirkungsvolle Strategie basiert auf neun elementaren Grundkomponenten: strategische Vision, Werte, strategisches Umfeld, strategische Absicht, strategische Konzeption, Teilziele und Bedingungen, Ressourcen, strategisches Controlling, eine Eventual- und Folgeplanung.
Die strategische Vision IKT-Sicherheit hat langfristig erreichbare, optimale Sicherheitszustände zu beschreiben, nicht den Weg zur Zielerreichung, und enthält keine Bewertungen hinsichtlich der Machbarkeit. Kern der Visionen muss der optimale Schutz der wesentlichen Grundwerte der IKT sein. Die jederzeitige Verfügbarkeit, angemessene Vertraulichkeit und unverletzliche Integrität (IKT-Grundwerte) der gewünschten Informationsdienste und Kommunikationswege der kritischen IKT, insbesondere die Hochverfügbarkeit der kritischen IKT-Infrastruktur (Richtung 100%), sind von vorrangiger Bedeutung.

Strategische Optionen für Österreich

Zum Schutz vor einem Cyber-Angriff bieten sich grundsätzlich folgende strategische Optionen[17)] an:
1. Prävention durch Abschreckung und Vorbeugung.
2. Verhinderung des Erreichens der politischen Ziele des Angreifers durch permanenten Schutz der kritischen Infrastruktur; dazu Notfall- und Krisenvorsorge.
3. Schadensbegrenzung; rasche Maßnahmen zur Begrenzung der Schadenshöhe.
4. Fähigkeit zur raschen Wiederherstellung geschädigter Systeme durch Krisenmanagement.
Die Prävention durch Abschreckung und Vorbeugung ist derzeit für Österreich keine Option, zumal dafür die Voraussetzungen fehlen, die Optionen 3 und 4 nehmen den Eintritt von großen Schäden in Kauf und sollten daher für einen selbstbewussten Staat auf dem Weg ins Informationszeitalter nicht akzeptabel sein. Die Option 2, nämlich die Verhinderung des Erreichens der Ziele durch den Angreifer durch permanenten Schutz der kritischen Infrastruktur und Notfall- und Krisenvorsorge, sollte jedenfalls angestrebt werden. Die Erfolgsaussichten dieser Option hängen überwiegend von den Besitzern und Betreibern der kritischen Infrastrukturen ab, zumal diese mit Masse in privater Hand sind.
Von staatlicher Seite ist auch im Cyber Space die Schutzfunktion gegenüber der Gesellschaft wahrzunehmen. Die Option 2 ist durch die Schaffung der Voraussetzungen, Rahmenbedingungen und Zurverfügungstellung der erforderlichen Ressourcen zielstrebig anzusteuern. Schutzobjekte sind dabei die kritischen, von IKT abhängigen Infrastrukturen des Landes.

Kritische Infrastrukturen

Kritische Infrastrukturen[18)] sind jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von staatlichen Einrichtungen.
Auf der Basis des Europäischen Programms für den Schutz kritischer Infrastrukturen[19)] wurde der Masterplan zur Erstellung des österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP = Austrian Program for Critical Infrastructure Protection) auf nationaler Ebene festgelegt. Der Masterplan beschreibt die Grundsätze des Programms, beinhaltet die Auflistung der vorrangig zu untersuchenden Sektoren, definiert Kriterien für die Einstufung kritischer Infrastrukturen, benennt die Risikofaktoren und die Akteure, listet die Maßnahmen zum Schutz kritischer Infrastrukturen auf und entwickelt einen Aktionsplan mit detaillierten Teilzielen.
Im europäischen Programm werden elf Sektoren kritischer Infrastrukturen[20)] angeführt: Energie, Nuklearindustrie, IKT, Wasser, Lebensmittel, Gesundheit, Finanzen, Transport, chemische Industrie, Raumfahrt und Forschungseinrichtungen.
Für Österreich sind nicht alle diese Sektoren von gleicher Bedeutung wie für die EU. Nuklearindustrie und Raumfahrt haben keine besondere nationale Bedeutung. Die Schwerpunkte bei der nationalen österreichischen kritischen Infrastruktur sollen hingegen auch die verfassungsmäßigen Einrichtungen, die Aufrechterhaltung des Sozialsystems und der Verteilungssysteme sowie die Hilfs- und Einsatzkräfte umfassen.
Die Zentralen, Kommunikationsknoten und Steuerungssysteme dieser, einer modernen Gesellschaft zu Verfügung stehenden kritischen Infrastrukturen basieren auf Informations- und Kommunikationstechnologie oder sind für die IKT von erheblicher Bedeutung und nur in bestimmten Objekten funktionsfähig.
Österreichs Transformation ins Informationszeitalter ist teilweise weiter fortgeschritten als jene Estlands.[21)] Österreich ist in erheblichem Ausmaß vom Funktionieren seiner kritischen Informationsinfrastrukturen abhängig. Während die Durchdringung mit IKT sehr rasch vorangeschritten ist, hinkt die Nachhaltigkeit durch einen Mangel an Absicherungsmaßnahmen hinterher.

Konsequenzen - Erforderliche Maßnahmen

Von staatlicher Seite sollte die Fähigkeit zum Schutz der strategischen IKT-Infrastruktur vor Cyber-Angriffen mittels eines ständig verfügbaren aktuellen Lagebildes auf der Basis regelmäßiger Analysen und Bewertung der Sicherheitsrisiken, eines Frühwarnsystems, ergänzt durch Notfalls-/Vorfalls-Funktionalitäten sowie durch die Fähigkeit zur angemessenen Reaktion, gestützt werden.
Eine intensive Zusammenarbeit auf nationaler Ebene zwischen Wirtschaft, Wissenschaft, Verwaltung und Bürgern (Private-Public-Partnership) ist zwingend geboten, von staatlicher Seite zu initiieren und zu fördern. Auf europäischer Ebene ist staatlicherseits insbesondere bei der Prävention, Bedrohungserkennung und Abwehr zu kooperieren.
Die Besitzer und Betreiber kritischer Infrastrukturen müssen durch umfangreiche Schutzmaßnahmen gegen Angriffe von außen und innen, Austausch von Informationen, Kooperationen zwischen den Betreibern, Einhaltung hoher Sicherheitsstandards und zertifizierte Ausbildung ihres Fachpersonals Voraussetzungen für den sicheren Betrieb schaffen. Entwicklung und Einsatz von intrusionstoleranten Systemen, redundante Auslegung, automatisierte und durch händische Steuerung überlagerte kritische Prozesse sind Ansätze zum Gelingen.
Für sicherheitskritische Bereiche sind ausschließlich akkreditierte bzw. zertifizierte Hard- und Software, Organisationen, Verfahren und verlässliche Personen einzusetzen. Schutzwürdige Daten sind gesetzeskonform, Objekte, abgestimmt auf die Kritikalität der IKT und den Grad der Bedrohung, zu schützen. Kritische Infrastrukturen erfordern einen permanenten Grundschutz mit aktiven und passiven Maßnahmen, mit Personal und Material. Dieser ist so auszulegen, dass bei vermuteter Gefahr durch Katastrophen, terroristische Anschläge oder Kriegshandlungen der Schutz rasch verstärkt werden kann.
Notfallpläne sind durch periodische Übungen aktuell zu halten, ein hohes Sicherheitsbewusstsein über die Risiken und erforderlichen Gegenmaßnahmen ist bei allen Beteiligten zu forcieren.
Die Absicherungsmaßnahmen sind grundsätzlich nach dem Motto „Schützen, entdecken, reagieren“ zu etablieren und in defensive und offensive Maßnahmen einzuteilen. Klar ist, dass IKT-Systeme eine besondere Rolle zur eigenen Information und Unterstützung in akuten und undurchsichtigen Lagen spielen.

Rechtlicher Anpassungsbedarf

Innerstaatlich ist im Bereich der vorbeugenden Abwehr und für die Bekämpfung von Angriffen aus dem Cyber Space auf „kritische IKT-Strukturen“ die Behördenzuständigkeit exakt festzulegen, die Organe sind mit den erforderlichen Befugnissen auszustatten. Um Missbräuchen vorzubeugen und die Akzeptanz dieser notwendigen Maßnahmen zu erhöhen, wäre ein effektiver Rechtsschutz- und Kontrollapparat vorzusehen.
Völkerrechtlich kann ein Angriff mit Mitteln der Informationstechnik vermutlich als „bewaffneter Angriff“ im Sinne der UNO-Charta qualifiziert werden.[22)] Bei der Qualifikation als „bewaffneter Angriff“ kommt es primär nicht nur auf das eingesetzte Mittel als solches an, sondern auf die Absicht der Schädigung und die Höhe des tatsächlichen Schadens. Da gerade auch mit Mitteln der Informationstechnik erhebliche Schäden verursacht werden können, die den Auswirkungen eines bewaffneten Angriffes um nichts nachstehen, könnten daher auch Angriffe aus dem Cyber Space durchaus als „bewaffneter Angriff“ im Sinne des Art. 51 der UNO-Satzung qualifiziert werden, die zur Ausübung des Rechts auf Selbstverteidigung legitimieren. Darüber hinaus wäre zu klären, welche Pflichten einem Neutralen obliegen, wenn über dessen „nationalen Cyber Space“ bewaffnete Angriffe gegen Dritte geführt werden.

Staatlicher Strukturbedarf

Von staatlicher Seite sind ausreichend Ressourcen für ein Instrument zur Analyse, Bewertung und Prognose von Entwicklungen der strategischen IKT einschließlich einer Risikobewertung, ein permanentes Lagezentrum zur Beobachtung und Bewertung der Bedrohungslage sowie für eine allfällige Frühwarnung, Alarmierung und Auslösung von Reaktionen und Notfallsorganisationen (CERT/CSIRT= Computer Emergency Response Team/Computer Security Incident Response Team) bereitzustellen.
Es bedarf einer zentralen Stelle in Österreich, die alle einschlägigen Informationen von Bundes- und Landesdienststellen sowie von Privaten sammelt, analysiert, bewertet und in der Lage ist, die notwendigen Aufklärungs-, Vorbeugungs-, Abwehr- und Reaktionsmaßnahmen zu treffen bzw. verbindlich anzuordnen. Diese Stelle hat auch zweckmäßigerweise die Steuerung und Koordination der nationalen und internationalen Zusammenarbeit sicherzustellen. Die erforderlichen gesetzlichen Voraussetzungen wären zu schaffen.

ANMERKUNGEN:
1) Vergleiche: „Overview of the cyber attacks against Estonia“ Version 0.2, Tallin 2007, nicht klassifiziertes NATO-Dokument, im Besitz des Verfassers.
2) DoS, DDoS: Als Denial of Service (DoS, zu Deutsch etwa: Dienstverweigerung) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service).
3) Bot, Botnet: Unter einem Bot (vom Begriff robot abgeleitet) versteht man ein Computerprogramm, das weitgehend autonom ständig gleichen, sich wiederholenden Aufgaben nachgeht. Es handelt sich dabei meist um ein eher simples, aber effektives Programm. Gebräuchlich ist die Bezeichnung auch für quasi-selbstständige Programme im Bereich der künstlichen Intelligenz. Kommunizieren Bots untereinander in einem fernsteuerbaren Netzwerk, so spricht man von einem Botnet. Dabei infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot, der sich dann zu einem IRC-Server verbindet, einen bestimmten Channel betritt und dort auf Befehle des Botnet-Besitzers, des so genannten Botmasters, wartet, wie beispielsweise das Starten eines DDoS-Angriffs oder das Versenden von Spam.
4) Spam: Als Spam oder Junk (englisch für „Abfall“ oder „Plunder“) werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und massenhaft versandt wurden oder werbenden Inhalt haben. Dieser Vorgang wird Spamming oder Spammen genannt, der Verursacher Spammer.
5) DNS: Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. In Analogie zu einer Telefonauskunft soll DNS bei Anfrage mit einem Hostnamen (dem „Adressaten“ im Internet - z.B. de.wikipedia.org) als Antwort die zugehörige IP-Adresse (die „Anschlussnummer“ - z.B. 91.198.174.2) nennen.
6) ping flood, syn flood, malformed GET queries sind Methoden zur Sabotage von Servern. Primitive DoS-Angriffe wie SYN-Flooding, PIH-Flooding oder die Smurf-Attacke belasten die Dienste eines Servers, beispielsweise HTTP, mit einer größeren Anzahl Anfragen, als dieser in der Lage ist zu bearbeiten, woraufhin er eingestellt wird oder reguläre Anfragen so langsam beantwortet, dass diese abgebrochen werden. Wesentlich effizienter ist es jedoch, wie bei WinNuke, mittels der Land-Attacke, der Teardrop-Attacke oder des Ping of Death Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese ebenso auf Anfragen nicht mehr reagiert.
7) Zombies: Als Zombie oder Drohne bezeichnet man einen am Internet angeschlossenen Computer, der durch Würmer, Viren, Trojaner, direkte Angriffe oder Ähnliches unter die Kontrolle eines Angreifers gebracht worden ist.
8) pps = packets per second.
9) Nashi: Jugendorganisation der Partei Haus Russland.
10) Vgl. „Overview of the cyber attacks against estonia“ Version 0.2, Tallin 2007, nicht klassifiziertes NATO-Dokument, im Besitz des Verfassers.
11) Vgl. Walter J. Unger/Heinz Vetschera: „Cyber War und Cyber Terrorismus als neue Formen des Krieges“. In: ÖMZ 2/2005, S.204ff.
12) Ebenda, S.203ff.
13) André Beaufre: Totale Kriegskunst im Frieden - Einführung in die Strategie, Berlin 1963, S.25.
14) Ebenda.
15) Vgl. Bundesamt für Sicherheit in der Informationstechnik: Internationale Aktivitäten zum Schutz kritischer Infrastrukturen, Bonn 2003, S.5ff.
16) Vgl. Ebenda S.6.
17) Vgl.: Lukasik, Goodman, Longhurst: „Protecting Critical Infrastructures Against Cyber-Attack“. In: ADELPHI PAPER 359, Oxford 2003, S.5ff.
18) Gemeinsamer Bericht des Bundeskanzlers und des Bundesministers für Inneres betreffend das österreichische Programm zum Schutz kritischer Infrastrukturen; Masterplan APCIP; Beschluss des Ministerrates vom 2. April 2008, S.1.
19) EPCIP = European Program for Critical Infrastructure Protection.
20) Vgl. a.a.O., Gemeinsamer Bericht des Bundeskanzler, S.5.
21) Österreich lag 2006 und 2007 im e-Government Ranking der EU auf Platz 1.
22) Vgl. Walter J. Unger/Heinz Vetschera: „Cyber War und Cyber Terrorismus als neue Formen des Krieges“. In: ÖMZ 2/2005, S.209ff.