Europäische Kommission
Vertretung in Luxemburg

Pressemitteilung

272-2010 – 30. September 2010

Kommission verstärkt Europas Abwehrmaßnahmen gegen Cyberangriffe

Die Europäische Kommission hat heute zwei neue Maßnahmen bekanntgegeben, mit denen Europas Verteidigungsfähigkeit gegen Angriffe auf seine wichtigsten Informationssysteme (IT) sichergestellt werden soll. Neben einem Vorschlag für eine Richtlinie über den Umgang mit neuen Arten der Cyberkriminalität wie etwa Cyber-Großangriffen legt sie einen Vorschlag für eine Verordnung vor, mit der die Europäische Agentur für Netz- und Informationssicherheit (ENISA) gestärkt und modernisiert werden soll. Beide Initiativen sind in der Digitalen Agenda für Europa und dem Stockholmer Programm vorgesehen, um das Vertrauen und die Netzwerksicherheit zu erhöhen. Aufgrund der vorgeschlagenen Richtlinie könnten die Urheber von Cyberangriffen sowie die Hersteller von damit in Verbindung stehender Software und Schadsoftware verfolgt werden und wären härteren strafrechtlichen Sanktionen ausgesetzt. Darüber hinaus wären die Mitgliedstaaten verpflichtet, im Falle von Cyberangriffen schnell auf dringende Hilfeersuchen zu reagieren. Die justizielle und polizeiliche Zusammenarbeit in Europa würde dadurch in diesem Bereich an Wirksamkeit gewinnen. Auch die Stärkung und Modernisierung der ENISA würde der EU, den Mitgliedstaaten und den privaten Akteuren dabei helfen, ihre Kapazitäten und Vorsorgemaßnahmen zur Prävention, Aufdeckung und Reaktion im Bereich der Internetsicherheit zu verbessern. Beide Vorschläge werden zur Verabschiedung an das Europäische Parlament und den EU-Ministerrat weitergeleitet.

Die für Inneres zuständige Kommissarin Cecilia Malmström sagte dazu: „Das Verbrechen geht neue Wege. Mithilfe von Schadsoftware ist es möglich, die Kontrolle über eine große Zahl von Computern zu gewinnen und Kreditkartennummern zu stehlen, sensible Informationen ausfindig zu machen und Großangriffe zu starten. Es ist an der Zeit, unsere Bemühungen gegen die häufig auch vom Organisierten Verbrechen genutzte Cyberkriminalität zu verstärken. Die Vorschläge, die wir heute vorlegen, sind ein wichtiger Schritt, weil wir damit die Erstellung und den Verkauf von Schadsoftware unter Strafe stellen und die europäische polizeiliche Zusammenarbeit verbessern."

Die für die Digitale Agenda zuständige Vizepräsidentin der Kommission, Neelie Kroes, erklärte: „Nur wenn die Bürger sich online wohl und sicher fühlen, werden sich auch alle Europäer im digitalen Raum bewegen. Online-Bedrohungen kennen keine Grenzen. Durch die Modernisierung der Europäischen Agentur für Netz- und Informationssicherheit wird neuer Sachverstand entstehen und der Austausch bewährter Praktiken innerhalb Europas gefördert. Unsere EU-Organe und Regierungen müssen sehr eng zusammenarbeiten, damit wir die Art und das Ausmaß der neuen Online-Bedrohungen verstehen lernen. Die ENISA muss uns mit Rat und Unterstützung dabei zur Seite stehen, effiziente Abwehrmechanismen zu entwerfen, um unsere Bürger und Unternehmen online zu schützen."

Auch wenn Europa darum bemüht ist, das Potenzial von Netzwerken und Informationssystemen voll auszuschöpfen, darf es dabei nicht anfälliger für Störungen durch zufällige oder natürliche Ereignisse (wie etwa Tiefseekabelbrüche) oder durch böswillige Handlungen (wie Hacker- oder sonstige Cyberangriffe) werden. Solche Angriffe könnten beispielsweise mithilfe immer ausgefeilterer Instrumente durchgeführt werden, mit denen eine große Zahl von Computern übernommen und zeitgleich als Roboterarmee im Internet („Botnets“) manipuliert werden können, ohne dass die Besitzer dies mitbekommen. Diese infizierten Computer können später benutzt werden, um vernichtende Cyberangriffe gegen öffentliche und private IT-Systeme zu führen - so geschehen in Estland im Jahre 2007, als die meisten öffentlichen Online-Dienste ebenso wie die Server der Regierung, des Parlaments und der Polizei vorübergehend außer Betrieb gesetzt wurden. Die Zahl der Angriffe auf Informationssysteme ist stetig gestiegen, seit die EU im Februar 2005 erstmals Regelungen über Angriffe auf Informationssysteme verabschiedete. Im März 2009 griff ein Netz infizierter Computer die Computersysteme staatlicher und privater Organisationen in über 100 Ländern an und verschaffte sich Zugang zu sensiblen und vertraulichen Dokumenten. Auch in diesem Fall erschuf Schadsoftware „Botnets“, also Netzwerke infizierter Computer, die ferngesteuert werden können, um einen koordinierten Angriff auszuführen.

Das heute von der Kommission vorgeschlagene Maßnahmenpaket wird Europas Abwehrkraft gegen Cyberstörungen stärken. Der Vorschlag der Kommission über Cyberkriminalität baut auf Regelungen auf, die seit 2005 gelten, und führt neue erschwerende Umstände und höhere strafrechtliche Sanktionen ein, die erforderlich sind, um die wachsende Bedrohung und Häufigkeit von Großangriffen auf Informationssysteme wirksamer zu bekämpfen.

Darüber hinaus würde damit der Weg für eine bessere Zusammenarbeit zwischen den Justiz- und Polizeibehörden der Mitgliedstaaten geebnet, indem die Mitgliedstaaten durch die Vorgabe, dringende Ersuchen innerhalb eines festgelegten Zeitrahmens zu bearbeiten, verpflichtet werden, das bestehende Netzwerk rund um die Uhr erreichbarer Kontaktstellen besser zu nutzen.

Schließlich würde die vorgeschlagene Richtlinie auch die Einrichtung eines Systems zur Erfassung und Rückverfolgung von Cyberangriffen vorsehen.

Verstärkte Zusammenarbeit unter Ländern und Industriezweigen

Zur besseren Koordinierung der europäischen Abwehrreaktionen schlägt die Kommission eine neue Verordnung vor, mit der die 2004 ins Leben gerufene Europäische Agentur für Netz- und Informationssicherheit (ENISA) gestärkt und modernisiert wird. Dadurch würde die Zusammenarbeit zwischen EU-Mitgliedstaaten, Strafverfolgungsbehörden und der Industrie intensiviert. Die ENISA wird bei der Stärkung des für die Entwicklung der Informationsgesellschaft wesentlichen Vertrauens eine wichtige Rolle spielen, indem sie die Sicherheit und Privatsphäre der Nutzer verbessert.

Mit ihrem neuen Mandat würde die ENISA EU-Mitgliedstaaten und Akteure des Privatsektors in europaweite gemeinsame Maßnahmen einbinden wie etwa Cybersicherheitsübungen, Public-Private-Partnerschaften für Netzwerkstabilität, Wirtschaftsanalysen und Risikobewertung sowie Sensibilisierungskampagnen.

Eine modernisierte ENISA wäre flexibler und anpassungsfähiger und stünde zur Verfügung, um EU-Staaten und -Organen Unterstützung und Rat in Rechtssetzungsfragen zu bieten.

Zu guter Letzt würde die vorgeschlagene Verordnung die größer gewordenen Herausforderungen im Bereich Internetsicherheit berücksichtigen, indem sie das Mandat der ENISA um fünf Jahre verlängern und ihre finanziellen und personellen Mittel schrittweise aufstocken würde. Die Kommission schlägt vor, auch die Führungsstruktur der ENISA zu stärken, indem die Aufsichtsrolle des Verwaltungsrats untermauert wird, in welchem die EU-Mitgliedstaaten und die Europäische Kommission vertreten sind.

Hintergrund

Die vorgeschlagene Richtlinie über Angriffe auf Informationssysteme hebt den Rahmenbeschluss 2005/222/JI des Rates auf. Die Mitgliedstaaten wären verpflichtet, der neuen Richtlinie über Cyberkriminalität nachzukommen und sie innerhalb von höchstens zwei Jahren nach ihrer Verabschiedung in innerstaatliches Recht umzusetzen.

Die ENISA wurde 2004 geschaffen, ihr derzeitiges Mandat läuft im März 2012 aus. Es wird nun vorgeschlagen, es um fünf Jahre zu verlängern. Diesem Verordnungsvorschlag ging ein umfassender Prozess voraus, zu dem eine Evaluierung der Agentur, Empfehlungen von deren Verwaltungsrat, zwei öffentliche Konsultationsverfahren und eine Folgenabschätzung einschließlich Kosten-Nutzen-Analyse gehörten.

Weitere Informationen

Homepage von Cecilia Malmström, EU-Kommissarin für Inneres:

http://ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_de.htm

Homepage von Neelie Kroes, für die Digitale Agenda zuständige Vizepräsidentin der Kommission

http://ec.europa.eu/commission_2010-2014/kroes/index_en.htm

Newsroom zur Informationsgesellschaft

http://ec.europa.eu/information_society/newsroom/cf/menu.cfm

Für weitere Auskünfte
Ernst Moutschen – 4301 32925
E-Mail: ernst.moutschen@ec.europa.eu