Verteidigung und Sicherheit der Informationssysteme

Frankreichs Strategie

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence Nationale
de la Sécurité
des Systèmes
d'Information

Vorwort

Wahrscheinlich haben wir noch nicht ganz alle das Ausmaß erkannt: im vom Staatspräsidenten im Juni 2008 vorgestellten *Weißbuch für Verteidigung und nationale Sicherheit*, erschien die Sicherheit der Informationssysteme, zusammen mit der Abschreckung, als ein Bereich, in welchem die Souveränität Frankreichs voll und ganz zum Ausdruck kommen sollte.

Der Cyber-Raum kann so als weit entfernt vom Bereich der Verteidigung und der nationalen Sicherheit erscheinen. In den letzten zwanzig Jahren hat die Digitaltechnik unser Privatleben und unser Berufsleben verschmolzen, die Wettbewerbsfähigkeit der Unternehmen auf ein bisher unbekanntes Niveau gehoben, die Behörden den Benutzern näher gebracht und die Transparenz der Funktionsweise der Institutionen unseres Landes begünstigt.

Der Cyber-Raum, als neuer Turm von Babel, ist ein Ort des Austausches der Weltkulturen, der Verbreitung von Ideen und Informationen in Echtzeit, und ein Ort des Austausches zwischen Personen.
Der Ausschluss aus der Digitaltechnik würde Einzelpersonen zur Einsamkeit, die Unternehmen zum Rückgang und die Nationen zur Abhängigkeit verdammen.

In der realen Welt sind die durch Kriege oder durch Terrorismus verursachten Zerstörungen wie auch die Ausschreitungen der Verbrecher sichtbar und werden oft in den Medien verbreitet. Im Cyber-Raum, einer abstrakten Welt, sind die Folgen von Cyber-Angriffen gegen die Informationssysteme der Staaten, der Unternehmen oder gegen die Computer der Bürger meistens nur von den Spezialisten sichtbar und werden der breiten Öffentlichkeit nicht bekannt.

Der Cyber-Raum, als neuen Thermopylen, ist ein Ort der Auseinandersetzung geworden: Aneignung persönlicher Daten, Auskundschaftung des wissenschaftlichen, wirtschaftlichen und kaufmännischen Vermögens von Unternehmen, die ihren Konkurrenten oder fremden Mächten zum Opfer fallen, Ausfall von Diensten, die für ein gutes Funktionieren der Wirtschaft oder des täglichen Lebens notwendig sind, Kompromittierung von souveräne Informationen und sogar, unter bestimmten Umständen, Verlust menschlicher Leben sind heute die potenziellen oder realen Folgen des Ineinandergreifens von Digitaltechnik und menschlicher Tätigkeit.

In Anbetracht des Vordringens des Cyber-Raums in den Bereich der nationalen Sicherheit und der dadurch drohenden Gefahren, hat die Regierung beschlossen, Frankreich mit einer strukturierten Verteidigungs- und Sicherheitskapazität zu versehen. So gründete sie im Jahre 2009 die Nationale Agentur für Sicherheit der Informationssysteme (Agence nationale de la sécurité des systèmes d'information = ANSSI), eine Behörde im Dienst der staatlichen Instanzen, der Unternehmen und der Bürger. Der Staatspräsident beschloss letzten Juli der Agentur, zusätzlich zu ihrer Sicherheitsaufgabe, eine Aufgabe der Verteidigung der Informationssysteme zu übertragen.

Ziel dieses Dokumentes ist es, die Leitgedanken der von Frankreich seit der Veröffentlichung des *Weißbuches für Verteidigung und nationale Sicherheit* verfolgten Strategie aufzuzeigen, um im Cyber-Raum die Sicherheit unserer Bürger, unserer Unternehmen und der Nation zu gewährleisten.

Francis DELON
Generalsekretär für Verteidigung
und nationale Sicherheit

Die von einem Sternchen gefolgten Wörter sind im Glossar definiert.

Fotos :

Deckblatt	Jean Mottershead (CC BY-NC-ND 2.0), oder frei von Rechten
Seite 11	Ruby MV (CC BY-NC-SA 2.0)
Seite 12	Simon BISSON (CC BY-NC-ND 2.0)
Seite 13	MrFenwick (CC BY-NC-ND 2.0)
Seite 14	Runran (CC BY-SA 2.0)

Inhaltsverzeichnis

Vorwort

Gesamtüberblick

Vier strategische Ziele

- Eine Weltmacht der Cyberverteidigung sein
- Die Entscheidungsfreiheit Frankreichs durch den Schutz der Informationen bezüglich der Staatssouveränität zu gewährleisten
- Die Cybersicherheit der kritischen nationalen Infrastrukturen zu stärken
- Die Sicherheit im Cyber-Raum zu gewährleisten

Sieben Handlungsachsen

- Vorausdenken, analysieren
- Erkennen, warnen, reagieren
- Unsere wissenschaftlichen, technischen, industriellen und menschlichen Fähigkeiten verstärken und deren Fortbestand gewährleisten
- Die Informationssysteme des Staates und der Betreiber von kritischen Infrastrukturen schützen
- Unser Recht anpassen
- Unsere internationale Zusammenarbeit ausbauen
- Kommunizieren, um zu informieren und zu überzeugen

Glossar

Gesamtüberblick

Unter den größten Bedrohungen für Frankreich in den nächsten fünfzehn Jahren wird im *Weißbuch über Verteidigung und nationale Sicherheit* von 2008 ein groß angelegter Cyberangriff gegen die nationalen Infrastrukturen angegeben.
Diese Feststellung hat die Regierung dazu bewogen, den Beschluss zu fassen, die nationalen Kapazitäten im Bereich der Cyberverteidigung in bedeutsamer Weise zu erhöhen. Die Gründung der Französichen Nationalen Agentur für Sicherheit der Informationssysteme (Agence nationale de la sécurité des systèmes d'information = ANSSI) im Jahre 2009 war der erste diesbezügliche Schritt.

Die im vorliegenden Dokument dargelegte nationale Strategie für Verteidigung und Sicherheit der Informationssysteme verkörpert die Ambition des *Weißbuchs*.
Die Strategie verfolgt vier Ziele.

1. Eine Weltmacht der Cyberverteidigung sein

Frankreich muss unter Beibehaltung seiner strategischen Autonomie die notwendigen Bemühungen unternehmen, um zum engsten Kreis der wichtigsten Nationen im Bereich der Cyberverteidigung zu gehören. So kommt uns die multiplizierende Wirkung der Zusammenarbeit zugute, und zwar sowohl auf praktischer Ebene als auch was die Einführung einer einheitlichen Strategie gegen gemeinsame Bedrohungen anbelangt.

2. Die Entscheidungsfreiheit Frankreichs durch den Schutz der Informationen bezüglich der Staatssouveränität zu gewährleisten

Die Regierungsbehörden wie auch die Akteure des Krisenmanagements müssen über Mittel verfügen, um in jeder Situation und mit aller Vertraulichkeit Kommunikation betreiben zu können. Die Netze, die diese Anforderung bereits erfüllen, müssen erweitert werden, unter anderem auf territorialer Ebene.

Die Vertraulichkeit der Informationen, die über diese Netze ausgetauscht werden, erfordert die Realisierung von vertrauensvollen Sicherheitsprodukten. Wir müssen die notwendigen Sachkenntnisse für ihre Entwicklung aufrechterhalten und die Entwicklungs- und Produktionsmethoden optimieren.

3. Die Cybersicherheit der kritischen nationalen Infrastrukturen zu verstärken

Die Funktionsweise unserer Gesellschaft ist immer mehr von Informationssystemen und Netzwerken, unter anderem dem Internet, abhängig. Ein gelungener Angriff gegen ein kritisches Informationssystem oder gegen das französische Internet kann schwerwiegende menschliche oder wirtschaftliche Folgen haben. Es ist wichtig, dass der Staat, in enger Verbindung mit den betroffenen Systemherstellern und Betreibern, daran arbeitet, die Sicherheit dieser kritischen Systeme zu gewährleisten und zu verbessern.

4. Die Sicherheit im Cyber-Raum zu gewährleisten

Die auf den Informationssystemen lastenden Bedrohungen betreffen sowohl die Verwaltungsbehörden als auch die Unternehmen und die Bürger.

Die Verwaltungsbehörde muss beispielhaft sein und den Schutz ihrer Informationssysteme und der Daten, die ihr anvertraut werden, verbessern.

Was die Unternehmen und die Privatpersonen anbelangt, muss Informations- und Sensibilisierungsarbeit geleistet werden.

Bezüglich der Bekämpfung der Cyberkriminalität wird Frankreich die Verschärfung des Rechts und die gegenseitige internationale Hilfe unterstützen.

Um diese Ziele zu erreichen, hat man sich für sieben Handlungsachsen entschieden :

1. In bezug auf das Umfeld besser vorausdenken und analysieren, um die passenden Entscheidungen zu treffen.
2. Die Angriffe erkennen und bekämpfen, sowie die potentiellen Opfer warnen und ihnen zur Seite stehen.
3. Unsere wissenschaftlichen, technischen, industriellen und menschlichen Fähigkeiten verstärken und deren Fortbestand gewährleisten mit dem Ziel, die notwendige Autonomie zu bewahren.
4. Die Informationssysteme des Staates und der Betreiber von kritischen Infrastrukturen schützen, um eine bessere nationale Widerstandsfähigkeit zu gewährleisten.
5. Unser Recht anpassen, um technologische Weiterentwicklungen und neue Anwendungen zu berücksichtigen.
6. Unsere internationale Zusammenarbeit im Bereich Sicherheit der Informationssysteme, Bekämpfung der Cyberkriminalität, sowie Cyberverteidigung ausbauen, um die nationalen Informationssysteme besser zu schützen.
7. Kommunizieren, informieren und überzeugen, um den französischen Bürgern die Möglichkeit zu geben zu erkennen, was bezüglich der Sicherheit der Informationssysteme auf dem Spiel steht.

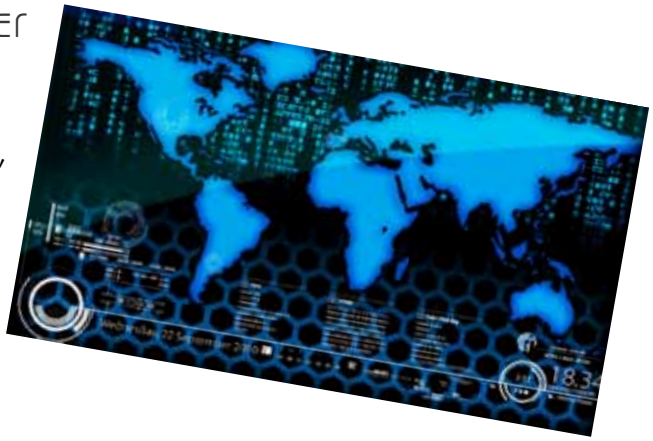
Dieses Dokument ist eine Zusammenfassung des öffentlichen Teils der durch das strategische Komitee für Sicherheit der Informationssysteme - eingerichtet durch die Verordnung Nr. 2009-834 vom 7. Juli 2009 zur Gründung der nationalen Agentur für Sicherheit der Informationssysteme (ANSSI) - bewilligten Zielsetzungen und Maßnahmen*.

„Frankreich muss einen Souveränitätsbereich bewahren, welcher sich auf die Kapazitäten konzentriert, die für die Aufrechterhaltung der strategischen und politischen Autonomie der Nation notwendig sind: die nukleare Abschreckung, der Bereich der ballistischen Flugkörper, die Jagd-U-Boote mit Atomantrieb, die Sicherheit der Informationssysteme, sind Teil dieses engsten Kreises."

„Verteidigung und nationale Sicherheit, Weißbuch", S.318

Vier strategische Ziele

I. Eine Weltmacht der Cyberverteidigung sein



Die Entwicklung der Informationsgesellschaft, welche durch die elektronischen Kommunikationsnetze gestützt wird, ist ein ungeheurer Antrieb für unser Wachstum, da sie wertschöpfend ist und zahlreiche Arbeitsplätze schafft. Sie trägt stark zur Wettbewerbsfähigkeit der nationalen Wirtschaftsstruktur, und somit zum Rang Frankreichs in der Welt bei.

Nun sind die elektronischen Netze unzulässigen Tätigkeiten ausgesetzt, welche direkt oder indirekt von Staaten durchgeführt werden. Einige üben über diese Netze massive Spionagetätigkeiten aus und versuchen Informationen bezüglich der Souveränität zu erhalten, zum Beispiel Informationen, welche Militärgeheimnisse sind, oder die zum wissenschaftlichen, technologischen, kaufmännischen oder finanziellen Vermögen der Unternehmen unserer strategischen Sektoren gehören.

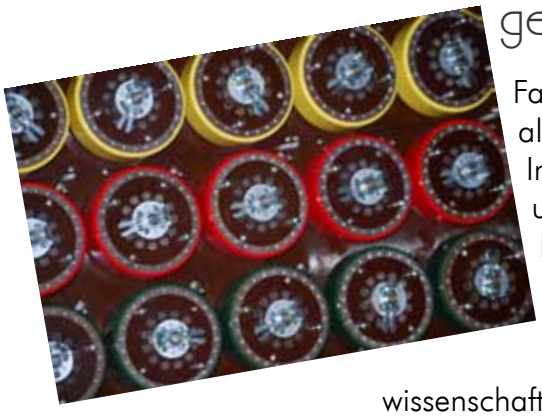
Terroristische Vereinigungen verwenden ihrerseits dieselben elektronischen Kommunikationsnetze, um ihre Ideen zu verbreiten, operationelle Informationen an ihre Organisation zu verteilen und Propagandatätigkeiten auszuüben.

In naher Zukunft wird es möglich sein, dass Staaten oder terroristische Vereinigungen die kritischen Infrastrukturen von Staaten angreifen, die als ideologisch feindlich angesehen werden.

Es ist folglich unbedingt notwendig, dass Frankreich über eine Cyberverteidigung verfügt.

Nun kennen die Auseinandersetzungen im Cyber-Raum im Gegensatz zu den Auseinandersetzungen in der konkreten Welt keine Grenzen. So kann eine glaubwürdige Cyberverteidigung nicht ausschließlich national sein, sondern sie muss sich auf ein Netz von Verbündeten stützen, mit welchen in Echtzeit ein Austausch von Informationen bezüglich der Schwachstellen, der Schutzvorrichtungen, der Angriffe und der gegenüber den im Cyber-Raum direkt oder indirekt von Staaten oder terroristischen Vereinigungen getätigten Attacken anzuwendenden Abwehrmittel möglich ist. Frankreich wird seine operationellen Partnerschaften mit seinen unmittelbaren Verbündeten verstärken, und sich auf seine Kompetenzen stützen, um aktiv zur Formulierung der Cyberverteidigungspolitik in den internationalen Organisationen beizutragen, unter anderem in der Europäischen Union.

2. Die Entscheidungsfreiheit Frankreichs durch den Schutz der Informationen bezüglich der Staatssouveränität gewährleisten



Falls die Entwicklung der Gesellschaft dazu tendiert, als Regel das Bestehen von Informationen sowie den Informationsaustausch und den zugleich augenblicklichen und in zahlreichen Formen möglichen Zugang zu Informationen einzuführen, besteht ein Teil des Gleichgewichtes der Welt nach wie vor in der Fähigkeit der Geheimhaltung der „Souveränitätsinformation", eines Teiles der diplomatischen, militärischen, wissenschaftlichen, technischen und wirtschaftlichen Information, welcher die Handlungsfreiheit ermöglicht und den Wohlstand der Nationen bedingt.

Wie schon in der Vergangenheit versuchen die Geheimdienste der ganzen Welt, sowie auch andere Akteure, die Souveränitätsinformation zu erhalten. Die Telekommunikationsnetze, unter anderem das Internet, die Informationen, die darin verbreitet werden, sowie die Informationen, die in den Netzen verfügbar sind oder in den Endgeräten, die sich daran anschließen, sind zugleich Informationsquellen und Informationssammler geworden.

Das effizienteste Mittel für den Schutz der Souveränitätsinformation ist die Verwendung der Verschlüsselung (Kryptographie*), welche das Begreifen der Information unmöglich macht oder zumindest verzögert, falls diese Information verändert, verbreitet oder abgefangen wird. Wegen der Fortschritte der Kryptoanalyse*, welche unter anderem denjenigen der Rechenleistung der Computer folgen, müssen Methoden und Techniken entwickelt und verwendet werden, die schwieriger zu analysieren sind und regelmäßig erneuert werden.

Die Aufrechterhaltung unserer strategischen Autonomie beruht auf unserer Fähigkeit die kryptographischen Techniken und Schlüsseltechnologien zu beherrschen, die für die Entwicklung von Sicherheitsprodukten*, die diese verwenden, nötig sind ; es muss folglich darauf geachtet werden, dass der Bereich der Sicherheit der Informationssysteme für junge Diplominhaber attraktiv bleibt, um den allmählichen Schwund der Kompetenzen zu vermeiden.

Parallel zur Notwendigkeit eine sichere und vertrauliche Kommunikation betreiben zu können, müssen die Entscheidungsträger wie auch die an der Krisenbewältigung beteiligten Dienststellen über Kommunikationsmittel verfügen, die unter allen Umständen bereitstehen. Diese sicheren elektronischen Austausch-, Fernsprech- und Videokonferenzmittel sind geplant und entwickelt worden. Ihre Verbreitung wird in den nächsten Jahren fortgesetzt, unter anderem zu Gunsten der Betreiber kritischer Bedeutung*.

3. Die Cybersicherheit der kritischen nationalen Infrastrukturen verstärken

Durch die Konvergenz verschiedener Technologien verflechten sich die Realwelt und die Netze. Zahlreiche Gegenstände der Realwelt — vom Supermarktetikett bis zur Raffinerie, vom Fotokopiergerät bis zur Kampfdrohne — weisen Informationssysteme auf und integrieren sich darin. Es ist möglich, durch diese Gegenstände übermittelte Informationen aus der Distanz über die Netze zu sammeln, ihren Betrieb aufrechtzuerhalten und sie anzusteuern.

Frankreich hat in seinem Verteidigungskodex Tätigkeitsbereiche von vitaler Bedeutung festgelegt, in welchen Betreiber tätig sind, die zur Deckung des für das Leben der Bevölkerungen unerlässlichen Bedarfs, zur Ausübung der Staatsgewalt, zum Wirtschaftsablauf, zur Aufrechterhaltung des Verteidigungspotentials oder zur Sicherheit der Nation beitragen, sofern diese Tätigkeiten nur schwer ersetzbar oder austauschbar sind.

Die meisten Betreiber vitaler Bedeutung verwenden in hohem Ausmaß Telekommunikationsnetze, insbesondere Internet, und zwar sowohl für ihre Verwaltung als auch für die Ausübung ihres Berufes. Jedoch sieht die Situation in diesem alten und dennoch neuen – weil durch die Zusammenschaltung der Systeme durcheinandergebrachten - Zusammentreffen zwischen der Industriewelt und der EDV-Welt folgendermaßen aus: die Industriewelt ist für die Sicherheit der Informationssysteme nicht ausreichend ausgebildet und sensibilisiert, und die EDV-Welt verkennt oft die Zwänge und die Funktionsweise der industriellen Systeme.

Die Abhängigkeit eines jeden Akteurs gegenüber dem Internet wird verstärkt durch schwere Tendenzen unserer wirtschaftlichen und sozialen Organisation: Outsourcing und Cloud Computing, Bündelung der Trägerdienste, Verwaltung in Echtzeit und schlanke Verwaltung, Nomadismus, Übertragung der Aufgaben auf die Kunden oder auf die Bürger, Schöpfung oder Umstrukturierung zahlreicher Prozesse.

Im Falle der Unterbrechung des Betriebs der Telekommunikationsnetze oder des Internets können sich die Ersatzmittel als völlig unzureichend erweisen, unter anderem durch fehlendes qualifiziertes Personal, welches in der Lage wäre die Prozesse aus der Zeit vor Beginn des Digitalzeitalters wieder in Betrieb zu setzen. Im Falle von Prozessen, die direkt aus neuen Anwendungen in Verbindung mit den Informationstechnologien stammen, gibt es keine Ersatzmittel.

Wie man regelmäßig in den Nachrichten aus aller Welt sehen kann, sind die möglichen Folgen von böswilligen Handlungen gegen die automatisierten Kontrollsysteme für Industrieprozesse, die von Betreibern vitaler Bedeutung eingerichtet werden, heute unzureichend abgeschätzt. So sind der Schutz der elektronischen Kommunikationsnetze – und unter anderem des Internet – wie auch die Sicherung der kritischen Systeme der

Betreiber vitaler Bedeutung nationale Prioritäten.

1. Die Sicherheit im Cyber-Raum gewährleisten

Für einen immer größeren Teil unserer Mitbürger prägt die Verwendung der elektronischen Kommunikationsnetze, wie zum Beispiel das Internet, die gängigsten Funktionen des Alltags, wie zum Beispiel die Funktionen in Verbindung mit dem Handel, mit Behördengängen oder mit dem Austausch zwischen Personen.

Parallel dazu sind die im Cyber-Raum von böswilligen Einzelpersonen oder Personengruppen verwendeten Techniken immer leistungsfähiger, und zielen darauf ab, Identitäten zu rauben, an die notwendigen Informationen für den Zugang zu Bankkonten zu gelangen oder persönliche Daten zu sammeln und zu verkaufen. Es sind ebenfalls immer mehr böswillige Remote-Kontrollübernahmen von Computern zu beobachten, um diese in Netze von kompromittierten Computern („Botnets*“) zu integrieren, die dazu da sind, unerlaubte Handlungen durchzuführen, wie zum Beispiel Cyberangriffe oder Versendung von böswilligen Emails.

In diesem Kontext müssen die Behörden ein Beispiel setzen, indem sie den öffentlichen Cyber-Raum schützen. Die Benutzer müssen die von den staatlichen Behörden angebotenen elektronischen Dienste vertrauensvoll benutzen können, unter anderem was den Schutz ihrer persönlichen Daten anbelangt. Das zu Beginn des Jahres 2010 veröffentlichte Allgemeine Sicherheitsbezugssystem* (référentiel général de sécurité = RGS) bietet einen Rechtsrahmen, welcher diese Sicherheit verstärken soll. Seine Einhaltung und seine Anwendung durch die staatlichen Behörden sind vorrangig.

Die Sicherung des Cyber-Raums wird durch eine systematische Information der Unternehmen und der Bürger bezüglich der Risiken und bezüglich der Mittel für den Schutz vor diesen Risiken erreicht. Ziel ist es, dass auf Dauer jeder Bürger im Laufe seiner Bildung bezüglich der Fragen der Cybersicherheit sensibilisiert werden kann. Dies erfordert die Einrichtung einer aktiven Regierungskommunikationspolitik.

Schließlich ist das Internet ein Rechtsraum. Frankreich muss die Verstärkung oder den Erlass von Rechtsvorschriften im Cyber-Raum fördern, wenn das bestehende Recht unzureichend ist, und die gegenseitige internationale Rechtshilfe bezüglich der Strafverfolgung bei Widerhandlungen in den elektronischen Kommunikationsnetzen oder über die elektronischen Kommunikationsnetze verstärken.

Für das Erreichen der vier strategischen Ziele wurden 7 Handlungsachsen definiert.

Sieben Handlungsachsen

1. Vorausdenken, analysieren

Gefahren und Bedrohungen entwickeln sich im Cyber-Raum schnell weiter. Das Erscheinen eines neuen Produktes oder einer neuen Softwareversion, die Veröffentlichung einer nicht korrigierten Sicherheitslücke* einer weit verbreiteten Software, das Auftreten einer neuen Technologie oder einer neuen Anwendung, eine politische Erklärung, können binnen kürzester Zeit eine Gefährdung der Sicherheit der Informationssysteme bewirken.

- In diesem Zusammenhang führen die Verteidigung und die Sicherheit unserer Informationssysteme in erster Linie über eine Verfolgung der Weiterentwicklungen der Technologien und über eine Analyse, über ein gutes Verständnis, ja sogar über einen Vorgriff auf das Spiel der öffentlichen oder privaten Akteure.

2. Erkennen, warnen, reagieren

In Anbetracht der steigenden Abhängigkeit der Unternehmen, der Infrastrukturen und der Dienste vom Internet, und auf Grund der durch einige Schwächen bedingten systemischen Risiken, ist es erforderlich, in der Lage zu sein, Sicherheitslücken und Angriffe so früh wie möglich zu erkennen, die potenziellen oder erwiesenen Opfer zu warnen und ihnen binnen einer kurzen Frist eine Hilfe für die Analyse und für die Ausarbeitung von Abwehrmitteln anzubieten.

- Wie im *Weißbuch für Verteidigung und nationale Sicherheit* vorgesehen, entwickelt Frankreich eine Kapazität für die Erkennung von Angriffen auf die Informationssysteme. Vorrichtungen, die unter anderem in den Netzen der Ministerien installiert sind, ermöglichen die Warnung ihrer Verantwortlichen, die Unterstützung bei der Identifizierung der Art der Angriffe und die Ausarbeitung passender Abwehrmittel.
- Um alle von den Erkennungstools und von den Überwachungsvorrichtungen gesammelten oder von unseren Partnern übermittelten Informationen zu verwalten, damit ein Bild in Echtzeit der Situation der nationalen Netze präsentiert werden kann und die Fähigkeit besteht, eine Krisensituation zu verwalten, legt sich die Nationale Agentur für Sicherheit der Informationssysteme (ANSSI) ein „Lagezentrum" zu, das Herausforderungen gewachsen ist.
- Um großen Krisen, welche die Sicherheit der Informationssysteme der Verwaltungsbehörden oder der Betreiber kritischer Insfrastrukturen beeinträchtigen

oder bedrohen, gegenüberzutreten, muss der Staat in der Lage sein, schnell die notwendigen Maßnahmen zu treffen. So gesehen übernimmt die ANSSI die Funktion der staatlichen Behörde für die Verteidigung der Informationssysteme.

3. Unsere wissenschaftlichen, technischen, industriellen und menschlichen Fähigkeiten verstärken und deren Fortbestand gewährleisten

Die Sicherheit der Informationssysteme beruht auf der Beherrschung von Technologie und auf praktisches Wissen, welches ebenfalls Organisationen und Einzelpersonen zugänglich ist, die diese Informationssysteme beeinträchtigen möchten. Auch wenn die staatlichen Akteure den Stand der Technik kennen müssen, müssen sie ebenfalls in der Lage sein, auf technologische Weiterentwicklungen vorzugreifen oder sie sogar zu erschaffen, und dabei die Forschungskapazitäten aufrechterhalten, die einzig und alleine den taktischen Vorteil des Angreifers gegenüber dem Verteidiger begrenzen können.

Frankreich verfügt über Forschungsteams von Weltniveau in den Bereichen der Kryptotechnik und der formalen Methoden. In weiteren Bereichen, wie zum Beispiel demjenigen der Sicherheitsarchitekturen von Informationssystemen, holt Frankreich das Niveau der am weitesten fortgeschrittenen Nationen ein.

- Um diese Arbeiten zu katalysieren, wird gerade die Gründung – zusammen mit industriellen Partnern – eines der Cyberverteidigung gewidmeten Forschungszentrums geprüft. Dieses Zentrum wird wissenschaftliche Forschungstätigkeiten durchführen (Forschung im Bereich der Kryptotechnik, Untersuchung der Angreifergruppen und ihrer Methoden, Gutachten bezüglich der Schadsoftware und der Sicherheitslücken, Entwicklung von gesicherter freier Software, Ausarbeitung von Konzepten für Verteidigung im Bereich der Informatik, usw.), sowie gutachterische und ausbildungstechnische Tätigkeiten.

Die Entwicklung der Informationsgesellschaft schafft für die Unternehmen einen auf Anhieb weltweiten Markt, auf welchem derzeit ein Vorverkaufsrecht für außerhalb Europas befindliche Akteure herrscht. Was die Sicherheit der Informationssysteme betrifft, ist diese Situation weder wünschenswert noch haltbar. Dabei verfügt Frankreich über eine in Europa einzigartige Spitzenindustriestruktur, welche es potenziell ermöglicht, einen großen Teil der für die Entwicklung von Sicherheitsprodukten notwendigen Technologien zu beherrschen, auch im Bereich der Bauteile. Zahlreiche innovative kleine und mittlere Unternehmen bilden diese Industriestruktur. Sie verfügen jedoch heute nicht über die notwendige kritische Größe und werden nicht durch eine ausreichende Nachfrage gestützt.

- Die industriellen Konsolidierungen werden durch die verschiedenen Mittel des Staates begünstigt, unter anderem durch die strategischen Investmentfonds.

Für eine bessere Effizienz müssen die Entwickler von Informatikprodukten und von Informationssystemen die Sicherheitsfragen gleich zu Beginn ihrer Entwicklungen berücksichtigen. Die Einbindung in die Industriestruktur von Experten für Sicherheit von Informationssystemen muss folglich verstärkt werden. Die Orientierung von jungen Leuten in Richtung dieser Berufe wird gefördert werden, um den nationalen Bestand an Kompetenzen zu vergrößern.

Allgemein müssen die wissenschaftlichen und technischen Ausbildungen im Bereich der Informationstechnologien die Sicherheit der Informationssysteme fachlich einbeziehen.

4. Die Informationssysteme des Staates und der Betreiber von kritischen Infrastrukturen schützen

Wie das *Weißbuch für Verteidigung und nationale Sicherheit* unterstreicht, müssen wir „über ein Angebot an völlig beherrschbaren Produkten allerhöchster Sicherheit für den Schutz der Staatgeheimnisse verfügen, sowie über ein Angebot an mit einem Gütesiegel versehenen Vertrauensprodukten und –diensten, auf welches die Behörden zurückgreifen werden, und das in hohem Maße dem Wirtschaftssektor zugänglich sein wird". Gesicherte widerstandsfähige* Netze müssen für „die gesamte Entscheidungs- und Befehlskette im Mutterland" verwendet werden.

- Im Bereich der geschützten Information* wurde die französische Strategie bezüglich der Sicherheitsprodukte und Bauteile neu definiert. Sie berücksichtigt unter anderem voll und ganz die Rückkehr Frankreichs in das integrierte NATO-Kommando.
- In den Ministeriumsnetzen wird die Einführung von starken Authentifizierungssystemen, welche zum Beispiel auf der Verwendung von Chipkarten – einem Bereich, in welchem Frankreich spezialisiert ist – beruhen, eine erhebliche Verbesserung der Sicherheit ermöglichen.
- Die staatlichen Behörden verfügen heute über ein gesichertes interministerielles Intranet, über ein Telefonnetz mit hoher Verfügbarkeit, welches bis 2012 voll und ganz mit neuen chiffrierten Endgeräten ausgestattet sein wird, und über eine geschützte Videokonferenzlösung, welche insbesondere dazu bestimmt ist, die ministeriellen Entscheidungsstellen auszurüsten. Die Einrichtung dieser verschiedenen Netze wird fortgesetzt, unter anderem in den territorialen Behörden.
- Im Bereich der Sicherheit der Informationssysteme der Betreiber kritischer

Infrastrukturen wird eine öffentlich/private Partnerschaft eingerichtet, um einerseits den Betreibern die Information zu Gute kommen zu lassen, über die der Staat bezüglich der Analyse der Bedrohungen verfügt, und es andererseits dem Staat zu ermöglichen, sicherzustellen, dass die für ein gutes Funktionieren der Nation wichtigen Infrastrukturen über ein passendes Schutzniveau verfügen. Es wird auch eine Zusammenarbeit mit den Systemherstellern erfolgen.

5. Unser Recht anpassen

Die durch die Entwicklung des Cyber-Raums bedingten neuen Anwendungen können, falls man nicht wachsam genug ist, Gefahren für unsere Privatsphäre, für das Funktionieren der kritischen Infrastrukturen oder für das Gleichgewicht unserer Unternehmen aufweisen.

Unser Gesetzgebungs- und Rechtsrahmen muss der Weiterentwicklung der Technik folgen. Die Texte werden in Abhängigkeit vom Auftreten neuer Technologien oder neuer Anwendungen angepasst, um die Sicherheit der Privatpersonen zu verstärken, und unter Berücksichtigung des Gleichgewichts zwischen dem Willen, so wenig wie möglich die Wettbewerbsfähigkeit der Unternehmen zu belasten, und der Notwendigkeit für den Staat, in der Lage zu sein, im Sinne des höheren Interesses der Nation einzugreifen.

- Was die Betreiber elektronischer Kommunikationen anbelangt, wird die Übertragung der europäischen Richtlinien in französisches Recht den Erlass neuer Regeln für den Schutz der Informationssysteme und für die Warnung der Regierungsbehörden bei einem Zwischenfall ermöglichen.
- Was die staatlichen Behörden anbelangt, werden die Umsetzung des « allgemeinen Sicherheitsbezugssystems » (référentiel général de sécurité = RGS) und seine Weiterentwicklung es ermöglichen, das Schutzniveau ihrer Informationssysteme erheblich zu erhöhen, unter anderem in ihren Beziehungen mit den Benutzern.

6. Unsere internationale Zusammenarbeit ausbauen

Die Sicherheit der Informationssysteme beruht zum Teil auf der Qualität des Informationsaustausches zwischen den zuständigen Diensten der verschiedenen Staaten. Frankreich wird darum bemüht sein, ein weitreichendes Netz an ausländischen Partnern einzurichten, um die gemeinsame Benutzung der wichtigsten Daten zu begünstigen, wie zum Beispiel der Informationen bezüglich der Schwachstellen oder der Sicherheitslücken der Produkte und Dienste.

Frankreich wird ebenfalls seinen Austausch mit den Partnern im Bereich der Bekämpfung der Cyber-Kriminalität intensivieren.

Auch bilden enge Beziehungen zwischen Verbündeten die Grundlage für eine effiziente Cyberverteidigung. Frankreich richtet einen sehr engen Kreis von Vertrauenspartnern ein, mit denen ein sehr tiefgreifender operationeller Austausch erfolgen wird.

7. Kommunizieren, um zu informieren und zu überzeugen

Die Sicherheit der Informationssysteme beruht sowohl auf der persönlichen Wachsamkeit als auch auf der Organisation, auf den Entscheidungen und den technischen Maßnahmen der Unternehmen und den Maßnahmen der Staaten.

In Anbetracht der potenziellen Konsequenzen eines Großangriffs gegen die Informationssysteme auf das Leben des Landes und seiner Bürger, müssen die Sensibilisierung und die Motivation der Personen und der Organisationen gewährleistet sein.

Nun müssen in Frankreich die Information und die öffentliche Diskussion über die durch die Beeinträchtigung der Sicherheit der Informationssysteme bedingten Bedrohungen der Verteidigung und der nationalen Sicherheit, oder einfach nur unseres täglichen Lebens, noch eine große Weiterentwicklung erfahren.

- Die ANSSI wird die Entscheidungsträger gezielt unterstützen, um ihnen dabei zu helfen, die Maßnahmen auszuarbeiten und die notwendigen Entscheidungen bezüglich der Sicherheit der Informationssysteme zu treffen, die für das gute Funktionieren ihrer Organisationen und für den Schutz ihres technischen, wissenschaftlichen, kaufmännischen oder finanziellen Vermögens wesentlich sind.
- Im weiteren Sinne wird von der ANSSI eine passende Kommunikation in Richtung Öffentlichkeit und Unternehmen entwickelt.

Glossar

Botnet

Ein botnet, oder anders ausgedrückt ein Roboternetz, ist ein Netz von Maschinen, welches einer böswilligen Einzelperson (Master) zur Verfügung steht. Dieses Netz ist so aufgebaut, dass sein Master Befehle an einen Teil oder an alle Maschinen des Botnets übermitteln kann und sie aktivieren kann, wie es ihm gefällt.

Bemerkungen: bestimmte Netze können eine beträchtliche Anzahl an Maschinen erreichen (mehrere Millionen). Diese können den Gegenstand eines illegalen Handels bilden oder für böswillige Handlungen gegen andere Maschinen verwendet werden.

Kryptoanalyse

Prozess der Entschlüsselung von geschützten Daten mittel Kryptographie, ohne in Besitz der Schlüssel zu sein.

Kryptographie

Disziplin, welche die Grundsätze, die Mittel und die Methoden für die Umwandlung von Daten beinhaltet, mit dem Ziel deren Inhalt zu verbergen, zu verhindern, dass ihre Änderung unbemerkt bleibt, bzw. ihre unerlaubte Benutzung zu verhindern (ISO 7498-2).

Kryptotechnik

Wissenschaft, welche die Kryptographie und die Kryptoanalyse einschließt.

Cyber-Kriminalität

Handlungen, die gegen die völkerrechtlichen Verträge oder gegen die nationalen Gesetze verstoßen, wobei die Netze oder die Informationssysteme als Mittel für das Begehen einer Straftat oder eines Verbrechens verwendet werden, oder selbst als Ziel verwendet werden.

Cyberverteidigung

Alle technischen und nichttechnischen Maßnahmen, die es einem Staat ermöglichen, im Cyber-Raum die als wesentlich betrachteten Informationssysteme zu verteidigen.

Cyber-Raum

Kommunikationsraum, welcher gebildet ist durch die weltweite Anbindung von Ausrüstungen für die automatisierte Verarbeitung digitaler Daten.

Cyber-Sicherheit

Für ein Informationssystem angestrebter Zustand, welcher es ihm ermöglicht, Ereignissen aus dem Cyber-Raum zu widerstehen, die die Verfügbarkeit, die Integrität oder die Vertraulichkeit der gespeicherten, verarbeiteten oder übermittelten Daten sowie der verbundenen Dienste, die diese Systeme anbieten oder zugänglich machen, gefährden könnten.

Die Cybersicherheit verwendet Sicherheitstechniken der Informationssysteme und stützt sich auf die Bekämpfung der Cyberkriminalität und auf die Einrichtung einer Cyberverteidigung.

Sicherheitslücke

Schwachstelle in einem Datenverarbeitungssystem, welche es einem Angreifer ermöglicht, den normalen Betrieb, die Vertraulichkeit oder die Integrität der Daten des Datenverarbeitungssystems zu beeinträchtigen.

Geschützte Information

Der Artikel 413-9 des Strafgesetzbuches gibt an, dass „die Verfahren, Gegenstände, Dokumente, Informationen, Datennetze, Computerdaten oder Dateien, deren Verbreitung oder deren Zugriff der Landesverteidigung schaden könnte oder zur Entdeckung eines Militärgeheimnisses führen könnte“ Schutzmaßnahmen unterzogen sind, die dazu bestimmt sind, ihre Verbreitung oder ihren Zugang einzuschränken.

Glossar

Netikette

Im Jahre 1995 durch die Internet Engineering Task Force (IETF) erstellte Charta, welche die Regeln des Anstands vorstellt, die für den im Cyber-Raum erfolgenden Austausch empfohlen werden (siehe Charta: http://tools.ietf.org/html/rfc1855 oder http://www.sri.ucl.ac.be/rfc1855.fr.html für eine französische Übersetzung).

Betreiber vitaler Bedeutung (opérateur d'importance vitale = OIV)

Der Artikel R. 1332-1 des Verteidigungskodex gibt an, dass die Betreiber vitaler Bedeutung unter den in Artikel L. 1332-1 desselben Kodex angegebenen öffentlichen oder privaten Betreibern ernannt werden, oder unter den in Artikel L. 1332-2 angegebenen Geschäftsführern.

Ein Betreiber vitaler Bedeutung:

- übt in Artikel R. 1332-2 angegebene und zu einem Tätigkeitsbereich vitaler Bedeutung gehörende Tätigkeiten aus;

- verwaltet oder benutzt im Rahmen dieser Tätigkeit ein oder mehrere Unternehmen oder bauliche Anlagen, eine oder mehrere Einrichtungen deren Beschädigung oder Nichtverfügbarkeit oder Zerstörung durch eine böswillige Handlung, durch eine Sabotagehandlung oder durch eine terroristische Handlung das Kriegs- oder Wirtschaftspotenzial, die Sicherheit oder die Überlebensfähigkeit der Nation direkt oder indirekt schwer belasten könnte, oder die Gesundheit oder das Leben der Bevölkerung in Frage stellen könnte.

Sicherheitsprodukt

Hardware oder Software, welche vorgesehen ist, um die Verfügbarkeit, die Integrität oder die Vertraulichkeit der gespeicherten, verarbeiteten oder übermittelten Daten sowie der verbundenen Dienste, die von den Informationssystemen angeboten oder zugänglich gemacht werden, zu schützen.

Widerstandsfähigkeit

In der Informatik handelt es sich um die Fähigkeit eines Informationssystems einem Absturz oder einem Cyberangriff zu widerstehen, und nach dem Störfall in seinen Ursprungszustand zurückzukehren.

Allgemeines Sicherheitsbezugssystem (référentiel général de sécurité = RGS)

Summe der von der ANSSI erstellten und von der Verordnung Nr. 2005- 1516 vom 8. Dezember 2005 vorgesehenen Regeln „bezüglich des elektronischen Austausches zwischen den Benutzern und den Verwaltungsbehörden, sowie zwischen den Verwaltungsbehörden", welche von bestimmten der Sicherheit der Informationen beitragenden Funktionen eingehalten werden müssen; zu diesen Funktionen gehören zum Beispiel die elektronische Unterschrift, die Authentifizierung, die Vertraulichkeit bzw. der Zeitstempel. Die Regeln, die in dem allgemeinen Sicherheitsbezugssystem (RGS) angegeben sind, müssen angewendet werden, und werden je nach dem von der Verwaltungsbehörde festgelegten Sicherheitsniveau angepasst, und zwar im Rahmen der Sicherung der Online-Dienste, für die es verantwortlich ist. Seine Erstellungs-, Genehmigungs-, Änderungs- und Veröffentlichungsbedingungen sind festgelegt durch die Verfügung Nr. 2010-112 vom 2. Februar 2010, welche der Anwendung der Artikel 9, 10 und 12 der in Verbindung mit der Sicherheit der auf elektronischem Wege ausgetauschten Informationen genannten Verordnung zu Grunde gelegt wurde. (siehe http://www.ssi.gouv.fr/rgs).

Sicherheit der Informationssysteme

Alle technischen und nichttechnischen Maßnahmen, die es einem Informationssystem ermöglichen, Ereignissen zu widerstehen, welche die Verfügbarkeit, die Integrität oder die Vertraulichkeit der gespeicherten, verarbeiteten oder übermittelten Daten sowie der verbundenen Dienste, die von diesen Systemen angeboten oder zugänglich gemacht werden, gefährden könnten.

Informationssystem

Organisierte Summe der Ressourcen (Hardware, Software, Personal, Daten und Verfahren), welche die Bearbeitung und die Verbreitung von Information ermöglichen.

A propos ANSSI

Die Nationale Agentur für Sicherheit der Informationssysteme (ANSSI) wurde am 7. Juli 2009 in Form eines Dienstes nationalen Zuständigkeitsbereichs gegründet.

Kraft der Verfügung Nr. 2009-834 vom 7. Juli 2009, geändert durch die Verfügung Nr. 2011-170 vom 11. Februar 2011, übernimmt die Agentur die Aufgabe der nationalen Behörde für Verteidigung und Sicherheit der Informationssysteme. Sie ist dem Generalsekretär für Verteidigung und nationale Sicherheit unterstellt, welcher dem Premierminister untersteht.

Mehr erfahren über die ANSSI und über ihre Aufgaben www.ssi.gouv.fr.

Februar 2011

Nationale Agentur für Sicherheit der Informationssysteme

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP - Frankreich
Webseiten : www.ssi.gouv.fr und www.securite-informatique.gouv.fr
E-mail : communication [at] ssi.gouv.fr