Trusted Computing

Sicherheit geht vor

[02.03.2012] Auch die IT-Systeme von öffentlichen Verwaltungen sind häufig Angriffen aus dem Netz ausgesetzt. Um hier Sicherheitsziele gewährleisten zu können, sollen künftig vermehrt Trusted-Computing-Technologien zum Einsatz kommen.

Das Jahr 2011 war das Jahr der Cyber-Kriminalität. Zahlreiche Fälle der gezielten Manipulation von Informationen, dem Ausspähen vertraulicher Daten und des Diebstahls von Identitäten haben die Verwundbarkeit von IT-Systemen gezeigt. Davon betroffen sind auch Regierungen und Verwaltungen. Unbeabsichtigt wird Angreifern durch meist kleine Schwachstellen oder Fehlkonfigurationen eine Hintertür geöffnet. Beeinträchtigt wird dadurch nicht nur die Funktionsweise eines technischen Systems, sondern in erster Linie das Vertrauen, das Bürger in die Verlässlichkeit des Informations- und Kommunikationsangebots der öffentlichen Verwaltung setzen. Auch kommunale IT-Entscheider müssen sich der Frage stellen, ob ihre Online-Angebote effektiv gegen Angreifer geschützt sind.

Komplexität als Fluch und Segen

Die zunehmende Komplexität moderner IT-Systeme ist dabei Fluch und Segen zugleich. Auf der einen Seite ermöglicht die Verknüpfung unterschiedlicher Fachverfahren eine neue Qualität in der kollaborativen Prozessbearbeitung und eine Effizienzsteigerung in der medienbruchfreien und nutzerorientierten Service-Erbringung. Andererseits ergeben sich durch die Vernetzung zusätzliche Bedrohungen für das Gesamtsystem.
IT-Sicherheit ist ein Querschnittsthema, bei dem es politische, ökonomische, organisatorische, rechtliche und technologische Aspekte zu beachten gilt. Damit ein IT-System seinen Zweck sicher erfüllt, müssen alle Bereiche bezogen auf das Gesamtsystem frei von Schwachstellen sein. Verlagerte Zuständigkeiten in der öffentlichen Verwaltung bewirken jedoch, dass selten ein Akteur alle Fäden in einer Hand hält und mehrere Ebenen überschaut. Der fehlende Überblick führt zu einem Informationsvakuum und zu Intransparenz. Deshalb liegt die Vermutung nahe, dass die meisten IT-Entscheidungsträger, die angeben, nie, selten oder gelegentlich Ziel von Angriffen zu sein, kaum wirklich über alle notwendigen Informationen zur Beurteilung der Sicherheitslage verfügen. Denn Grundlage für die Beurteilung des Risikos ist die Kenntnis der Bedrohung. Es reicht nicht aus, sich darauf zu verlassen, dass jeder Vorfall bemerkt wird. Zudem ist es objektiv schwierig, auf technischer Ebene alle real geführten Angriffe zu erkennen.

Latent unsichere IT-Systeme

Eine weitere Ursache für latent unsichere IT-Systeme ist der Einsatz von gängigen Web Frameworks wie Drupal, Wordpress und TYPO3. Insbesondere von kleinen Internet-Agenturen realisierte Portale sind stark an der gewünschten Funktionalität des kommunalen Auftraggebers orientiert und vernachlässigen Sicherheitsbetrachtungen aus Kostengründen und aufgrund fehlender Sensibilisierung. Besonders gefährlich sind hier so genannte ungepatchte Monokulturen. Unter den Begriff fallen unter anderem Content-Management-Systeme, bei denen notwendige Sicherheitspatches nicht zeitnah eingepflegt werden. In diesen weit verbreiteten und auch im öffentlichen Sektor beliebten Systemen besteht ein erhöhtes Gefährdungspotenzial, da Angreifer automatisiert erkennen, ob notwendige Sicherheitspatches vergessen oder nicht zeitnah eingepflegt wurden. Ein anderes Problem sind Passwörter. Für diese werden

in einigen Web Frameworks keine ausreichenden Sicherheitsmaßnahmen vorgegeben. Ohne entsprechend nachgerüstete Module können die Kennungen in kurzer Zeit entschlüsselt werden.

Was ist Trusted Computing?

Einen Paradigmenwechsel in der IT-Sicherheit öffentlicher Verwaltungen kann mittelfristig die von der Trusted Computing Group (TCG) entwickelte Trusted-Computing-Technologie einläuten. Sie wird als nachhaltig und kosteneffizient eingestuft. Bei diesem Prinzip wird die Ausführung von Basissystem und Anwendungen in einem vertrauenswürdigen Zustand vermessen (Referenzmessung). Vor jedem Start wird das ausführbare Programm einschließlich der Umgebungsparameter erneut gemessen und abgeglichen. Bei einer schadhaften Veränderung stimmen die Messungen nicht mehr überein – das System wird als nicht mehr vertrauenswürdig behandelt. Der bei jedem Neustart des Systems für jede Software-Ebene durchgeführte Trusted-Computing-Mechanismus wird durch ein Hardware-Modul (Trusted Platform Module) und eine starke Kryptografie abgesichert.
Der Einsatz von Trusted-Computing-Systemen ist eine Schutzmaßnahme, die heute von kaum einer Verwaltung umgesetzt wird. Perspektivisch wird sich dies durch die in Windows 8 integrierten Trusted-Computing-Mechanismen ändern, die das Prinzip massenhaft verfügbar und verkehrsüblich machen werden. Damit wird es für Cloud-Service-Anbieter möglich, die von der öffentlichen Stelle benötigten Kontroll- und Steuerungsmöglichkeiten online zur Verfügung zu stellen, um den Anforderungen der Auftragsdatenverarbeitung gerecht zu werden. Andererseits wird es Bürgern als Nutzern möglich sein, online zu prüfen, ob sich die Services der Verwaltung in einem Zustand befinden, der von einer externen Prüfinstanz als vertrauenswürdig eingestuft wurde.

Regemäßige Sicherheitstests

Das Unternehmen init empfiehlt öffentlichen Stellen, sich bei der Erstellung von Ausschreibungsunterlagen bis zur Umsetzung ihrer IT-Verfahren am aktuellen Stand der Technik bezüglich vertrauenswürdiger Infrastrukturen zu orientieren. Das Engagement darf jedoch nicht mit der Inbetriebnahme der Plattform enden. Ist das Portal erst einmal online, sollte es regelmäßig automatisiert getestet werden. Dabei kann der einem Viren-Scan ähnliche Testablauf entlang mittlerweile gut kategorisierter Gefahrenschwerpunkte durch einen externen Dienstleister erfolgen, der die Sicherheits- und Datenschutzanforderungen der veröffentlichten E-Government-Dienste sehr gut kennt. init bietet hierfür zum Beispiel im Rahmen eines Security-Engineering-Prozesses drei abgestufte IT-Sicherheitstests an.
Im Unterschied zu Kraftfahrzeugen ist die ASU für Internet-Portale weitaus komplizierter, da es zwar eine limitierte Anzahl verschiedener Autotypen gibt, aber nahezu jede Website ein Einzelfall ist. Letztlich ist die Politik gefragt, durch sinnvolle Verbindlichkeiten dazu beizutragen, dass ein annehmbares Sicherheitsniveau informationstechnischer Systeme in Bund, Ländern und Kommunen gewährleistet ist.

()

Stichwörter: IT-Sicherheit, Trusted Computing, Datensicherheit, Datenschutz