Schutz auf Knopfdruck

Gemeinsam stark gegen Cyber-Angriffe

Cyber-Bedrohungen lassen IT-Verantwortliche nicht mehr ruhig schlafen. Weltweite Steuersünderkarteien, anonym veröffentlicht, Trojan.Hydraq, Duqu, Flame und auch der schon in die Jahre gekommene Stuxnet-Wurm Conficker greifen immer noch erfolgreich die Netze an und stehlen Daten. Öffentliche Auftraggeber haben hochwertige Datenbestände und sind deshalb häufig das Ziel von Angriffen. Wie sehen die Mindestanforderungen an eine sichere IT aus dem Public Sector aus?

Von Ramon Mörl, itWatch GmbH

Die Piraten des 21. Jahrhunderts sind Datenpiraten und stehlen zu verschiedensten Zwecken und mit unterschiedlichen Motivationen qualitativ hochwertige Informationen. Wegsehen hilft nicht, wenn es um den Schutz dieser Daten vor den Cyberkriminellen geht. Beinahe täglich gibt es Nachrichtenmeldungen über neue Bedrohungen. Allen gemeinsam ist, dass organisatorische Richtlinien dagegen nicht helfen, denn kein Anwender sieht einer URL oder einem Datenträger an, ob darin Malware enthalten ist. Es ist also zwingend notwendig, organisatorische Maßnahmen auch technisch zu untermauern.

Nicht zuletzt aus diesem Grund arbeitet das Bundesinnenministerium an einem Gesetz zur Einführung von Mindestsicherheitsstandards und zur Erhöhung der Sicherheit informationstechnischer Systeme speziell für kritische Infrastrukturen. Die öffentliche Verwaltung ist davon direkt betroffen.

Die Cyber-Angriffe, mit denen es Behörden zu tun haben, sind komplex. Deshalb erfordert es eine geschickte Kombination von Ressourcen, die Abwehrmaßnahmen Tag für Tag aktuell zu halten und darüber hinaus eine IT-Sicherheitsarchitektur zu implementieren, die kein Stückwerk darstellt, sondern systematisch aufgebaut ist und langfristigen Bestand hat. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Branchenverband BITKOM haben deshalb die Allianz für Cyber-Sicherheit [1] gegründet, um Informationen und Abwehr-Know-how zu bündeln und für die Gemeinschaft geeignet verfügbar zu gestalten. itWatch ist Partner dieser Cyber-Allianz und bringt dort ein benutzerfreundliches Verschlüsselungswerkzeug ein, „PDWatch2Go". PDWatch2Go – „PD" steht dabei für „private Daten" – kann unter „BSI für Bürger" kostenfrei für die private Nutzung heruntergeladen werden [2].

Für die Behörden lösen sich die Probleme der Cyber-Angriffe natürlich nicht durch den Kauf oder das Installieren eines einzelnen Produkts. Sinnvoller wäre eine – möglichst über Verbände oder andere Dachorganisationen abgestimmte und im besten Fall auch zertifizierte – umfassende Lösung, die alle Hauptanforderungen abdeckt. itWatch kooperiert deshalb intensiv mit mehreren Industriepartnern, zum Beispiel mit genua als dem Hersteller der vom BSI nach Common Criteria in der Stufe EAL 4+ zertifizierten Firewall genugate und mit T-Systems als einem Integrator für „fertige" Lösungen der IT-Sicherheit. Das gemeinsame Ziel ist es, einen „Schutz auf Knopfdruck" herzustellen, so dass nicht jeder IT-Betreiber das komplexe Know-how aus allen Bereichen selbst sammeln und aktuell halten muss – für Themen wie Applikations-, Geräteschnittstellen- und Druckkontrolle, für sicheres Löschen, Monitoring, die Inhaltskontrolle des Datentransfers auch in die Cloud, Virtualisierung und die Verschlüsselung mobiler und lokaler Daten sowie von Informationen in der Cloud. Vor allem aber soll es möglich sein, von vornherein eine sichere Basiskonfiguration für alle Standardanforderungen auszuliefern.

Standards sichern das Niveau

Angriffe erfolgen immer auf das schwächste Glied in einer Sicherheitskette. Deshalb hilft es niemandem, wenn eine einzelne Kommune unter Sicherheitsgesichtspunkten alles richtig gemacht hat, ein Angriff dann aber von der Nachbarkommune „herüberschwappt", die sich nur auf organisatorische Maßnahmen verlässt. Hier kommen wieder die Standards ins Spiel, denn man muss sich auf die Partner verlassen können, die zusammen in einem Netz agieren. Dafür legt man die gemeinsamen Spielregeln fest. Eine dieser Spielregeln lautet, dass nicht jeder „auf seiner Seite machen kann, was er will", sondern

Weiterführende Informationen

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/Startseite.html

[2] https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Links/links_node.html

IT-Sicherheit verlangt nach Spielregeln (Bild: Fotolia.com).

dass eine wichtige Einschränkung greift: Jeder ist in seinem Vorgehen frei, solange er die vereinbarten Mindeststandards einhält.

Anwender selbst können ihr IT-Sicherheitsmanagement nach ISO 27001 oder BSI Grundschutz zertifizieren lassen, um nachzuweisen, dass sie Mindeststandards einhalten. Bei Herstellern sind es vor allem Zertifizierungen wie die nach Common Criteria oder gewonnene Ausschreibungen von Bundesbehörden, die sie als akzeptablen Partner erkennbar machen. Bei itWatch war es beispielsweise der Rahmenvertrag zur Lieferung von Software zur Schnittstellenkontrolle an sämtliche Bundesbehörden, der die Einhaltung des erforderlichen Sicherheitslevels bestätigte.

In der IT-Sicherheit gilt es bei der Produktauswahl mindestens zwei Aspekte zu berücksichtigen: Den Funktionsumfang eines Sicherheitssystems und dessen Robustheit, also die Stärke der Funktionen gegen Angriffe. Beim Nachweis der Robustheit verlässt man sich am besten auf die Testergebnisse von dafür eigens aufgebauten Organisationen wie zum Beispiel dem BSI oder auch den Labors bei den TÜVs. Auf solcher Grundlage hat zum Beispiel die BWI Informationstechnik GmbH für den zentral verwalteten Betrieb von 140.000 Arbeitsplätzen der Bundeswehr an mehr als 1000 Standorten Produkte von itWatch für Umgebungen bis Schutzklasse VS-NfD und für einige tausend Arbeitsplätze bis Schutzklasse GEHEIM bestellt. Inzwischen hat auch die Bundespolizei mit einem Roll-Out begonnen.

Niemals gegen die Mitarbeiter

Zuletzt bleibt immer noch der Faktor Mensch. Es ist nicht möglich – oder sehr teuer – und meistens auch nicht sinnvoll, IT-Sicherheit gegen die Mitarbeiter durchzusetzen. Ratsam ist es, sichere Handlungsräume für die Mitarbeiter zu schaffen, ohne diese in der Ausübung ihrer Tätigkeiten einzuschränken.

Es hat sich in vielen Projekten bewährt, in der Einführungsphase einer Security-Lösung die Mitarbeiter durch Hinweistexte einzubinden, die immer dann in Echtzeit erscheinen, wenn sie eine sicherheitskritische Handlung vornehmen wollen. So werden die Mitarbeiter für aus Sicherheitsgründen modifizierte Vorgehensweisen sensibilisiert. Sie können sich auf die anstehende Veränderung einstellen und die für ihre Tätigkeiten eventuell notwendigen Berechtigungen beantragen. Am Ende der Einführungsphase entsteht auf diese Weise ein Mehr an Sicherheit, ohne die Anwender unnötig einzuschränken und ohne dass das Aufkommen an Helpdesk-Anrufen steigt. Im weiteren Verlauf bindet man die Mitarbeiter am besten in kritischen oder rechtlich relevanten Situationen weiterhin über Dialoge ein, welche später auch für ein eventuelles Audit für die notwendige Nachvollziehbarkeit und bei Bedarf Beweisbarkeit sorgen.

Viele Vorfälle legen es nahe, die Zugriffsberechtigungen für lokale und Domänen-Administratoren einzuschränken – auch deshalb, um diesen Personenkreis von einem Generalverdacht freizusprechen.

Verschlüsselung – pragmatisch gelöst

In vielen IT-Umgebungen bei öffentlichen Auftraggebern werden äußerst kritische personenbezogene Daten auf einzelnen Rechnern gehalten – dies trifft beispielsweise für kommunale Kindergärten und Sozialeinrichtungen zu. Daten auf Einzelcomputern finden sich außerdem bei der Verarbeitung von Micro-Zensus-Dateien und etwa dann, wenn medizinische Informationen über Arbeitnehmer oder Familien in sozialen Brennpunkten oder Konfliktbereichen aufzunehmen sind. Häufig tauschen die zuständigen Mitarbeiter und die Betroffenen überdies entsprechende Informationen per Mail oder mobile Datenträger aus.

Die Verschlüsselungslösung von itWatch schafft hier nicht nur die Möglichkeit, dass jeder Nutzer Daten sicher – also verschlüsselt – mitnehmen und weitergeben kann, sondern auch die Voraussetzung, Daten lokal oder in der Cloud verschlüsselt abzulegen. Eine Verschlüsselung für einen definierten Benutzerkreis ist ebenfalls möglich. So können Behörden und Bürger ohne gemeinsame Infrastruktur und ohne Kauf von zusätzlichen Lizenzen auch über moderne Plattformen wie die Cloud sicher kommunizieren.

Fazit

Gemeinsames Handeln auf nationaler Ebene und das Vereinbaren, Erreichen und Einhalten eines gemeinsam definierten technisch unterstützten Schutzniveaus sind die Gebote der Stunde, um Cyber-Angriffen nachhaltig Paroli zu bieten. Der Angreifer versteckt sich meist gut – deshalb benötigt man immer auch technische Analysemittel, um zu sehen, „was wirklich drin ist“. ■

Man weiß nie, wo sich der Angreifer versteckt (Bild: Fotolia.com).