Netzwerksicherheit

Grundregeln einhalten

[02.11.2016] Die Zahl der Angriffe auf Behördennetzwerke nimmt stetig zu. Sicherheitsprobleme entstehen oft durch Nachlässigkeiten und organisatorische Mängel. Wer gewisse Grundregeln einhält, kann die Risiken für einen erfolgreichen Cyber-Angriff daher deutlich minimieren.

Auf der vierten Potsdamer Konferenz für Nationale CyberSicherheit des Hasso-Plattner-Instituts stellte Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz, die Frage: Ist die Cyber-Welt die Achillesferse westlicher Nationen? Um sie gleich darauf mit den Worten „Ich fürchte ja“ zu beantworten und zu konstatieren: „Wir hängen ab vom Netz, wir hängen am Netz“. Doch es gibt Möglichkeiten, ein Netz, sei es ein Unternehmensnetzwerk, ein Behördennetzwerk oder das Netz des Deutschen Bundestags, zu schützen und das Risiko für einen erfolgreichen Cyber-Angriff zu minimieren.

Angriffe werden gezielter

Der Handel mit Daten aus Cyber-Angriffen ist ein lukratives Geschäftsfeld, in dem große Summen umgesetzt werden. Dementsprechend steigt die Professionalität, die Angriffe werden gezielter. Öffentliche Verwaltungen waren in Deutschland früher kein attraktives Ziel für Hacker, weil wirtschaftlich eher uninteressant. Doch inzwischen sind professionelle Hacker auch an Meldedaten, Steuerdaten, Polizei- oder Justizdaten interessiert. Durch die steigende Verbreitung von mobilen Geräten wie Smartphones und Tablets kommen neue Gefahrenquellen hinzu.
Allein in den Netzen von Hamburg und Schleswig-Holstein wehren die Sicherheitssysteme von Dataport Monat für Monat rund tausend Angriffe durch Schadprogramme ab. Dazu gehören Trojaner, Viren, Adware, Remote-Verwaltungs-Tools, Kennwort-Cracker, Scherzprogramme, Spam-Programme und viele mehr. Täglich werden weltweit über 100.000 neue Schadprogramme entwickelt. Fast 440 Millionen solcher Programme sind bereits bekannt. Das CERT (Computer Emergency Response Team) des Bundesamts für Sicherheit in der Informationstechnik (BSI) gibt jeden Monat über 200 neue Warnungen heraus, aufgrund derer durchschnittlich zwölf Sicherheitslücken in der IT-Infrastruktur geschlossen werden.

Gefahren reduzieren

Oftmals unterschätzt werden auch Sicherheitsprobleme durch die eigenen Mitarbeiter, meist durch Nachlässigkeiten und organisatorische Mängel. Die Klassiker: Mitgebrachte Speichermedien wie USB-Sticks schleusen Malware ein. Passworte werden nicht regelmäßig geändert oder sind leicht zu erraten. Zugangsdaten werden auf Zettel notiert und an die Urlaubsvertretung weitergegeben. Es werden ohne strikte Regeln Zugänge an vertrauenswürdige Gäste oder Externe vergeben. Diese Gefahren lassen sich auf ein Minimum reduzieren. Den Weg dazu geht Dataport seit Jahren konsequent, er lautet: Standardisierte Endgeräte, striktes Management, aktuelle Software, klare Organisation und hohes Sicherheitsbewusstsein. Mit diesen fünf Grundsätzen lässt sich ein Maximum an Sicherheit in jedem Behördennetzwerk gewährleisten.
Denn zentral gemanagte Computer mit Standardkonfigurationen sind deutlich weniger anfällig gegen Schad-Software als frei konfigurierte Computer. Dataport betreibt rund 70.000 Arbeitsplätze in den Verwaltungen der Länder Hamburg, Bremen und Schleswig-Holstein nach einem Standard. Die standardisierten Endgeräte erweisen sich als besser geschützt als andere, da bei ihnen zum Beispiel das

Ausführen von Programmen unterbunden oder auf bestimmte Bereiche beschränkt werden kann. So hat etwa der Verschlüsselungstrojaner TeslaCrypt, der bis 2016 grassierte, kein einziges der von Dataport zentral gemanagten Endgeräte befallen.
Ein weiterer Grundsatz: Software darf erst dann in Netzwerken eingesetzt werden, wenn sie eingehend auf ihre Sicherheit überprüft wurde. Zu einem strikten Software-Management gehört auch, nicht benötigte Dienste von Betriebssystemen zu deaktivieren. So werden viele potenzielle Einfallstore für Schad-Software geschlossen. Darüber hinaus müssen mittels Patches und Updates die entdeckten Sicherheitslücken in Programmen möglichst schnell auf allen Endgeräten im Netz geschlossen werden. Zudem gilt es, laufend Warnhinweise zu verarbeiten, Schwachstellen abzusichern und Patchreports auszuwerten.

Regeln auch einhalten

Für den sicheren Betrieb eines Netzwerks sind außerdem klare Regeln und transparente Strukturen zwingend nötig. Netzwerksicherheit ist zum erheblichen Teil eine organisatorische Angelegenheit. Rechte und Pflichten von Benutzergruppen sind klar zu beschreiben und einzuhalten. Sicherheitskritische Ereignisse sollten nach präzise definierten Standards erkannt und behandelt werden. Die besten Sicherheitssysteme sind wenig wert, wenn sie nicht durch starke organisatorische Strukturen und Regeln begleitet werden. So sorgt zum Beispiel eine strenge Passwortrichtlinie dafür, dass jeder Nutzer nach einigen Wochen seine Passworte in ausreichender Komplexität erneuern muss. Das ist lästig, steigert die Sicherheit aber beträchtlich.
Wesentliche Sicherheitsfaktoren stellen zu guter Letzt das Einhalten von Sicherheitsvorschriften und ein gesundes Misstrauen dar. Denn die Nachlässigkeit der Nutzer ist die größte Gefahr für Unternehmensnetzwerke. Das Einhalten sicherheitsrelevanter Prozesse und Regeln und eine gewisse Wachsamkeit für Unregelmäßigkeiten müssen fester Bestandteil der Unternehmenskultur sein. Bei Dataport wurde in den vergangenen Jahren das Sicherheitsbewusstsein intensiv weiterentwickelt. Die Folge: Die Mitarbeiter sind deutlich aufmerksamer geworden und melden auf hohem Niveau immer qualifizierter Ereignisse, die sicherheitskritisch sein könnten. Dagegen ist die Zahl der tatsächlich eingetretenen Sicherheitsvorfälle rückläufig.

Konsolidierung bringt Sicherheit

Es wird deutlich: IT- und Datenschutz benötigen ein professionelles IT-Sicherheitsmanagement. In Kooperation mit anderen oder durch Nutzung leistungsfähiger Dienstleister lassen sich die notwendigen Strukturen und das Know-how aufbauen. Und noch ein weiterer Aspekt hat große Relevanz: Konsolidierung. So hat etwa der Bund begonnen, seine IT zu konsolidieren und zielt damit auf IT-Sicherheit. Zudem will er die Hoheit und Kontrollfähigkeit über seine Informationstechnik erhalten. Eine Strategie, die Dataport mit seinen Trägern bereits erfolgreich umgesetzt hat. Mit der Konsolidierung der Rechenzentren auf zwei redundant ausgelegte Systemräume an zwei Standorten steht den Trägern von Dataport eines der sichersten Rechenzentren Europas zur Verfügung, das vom BSI und von der TÜV Informationstechnik (TÜViT) zertifiziert wurde.
Mit den genannten Grundsätzen sowie dem gemeinsamen Betrieb hochsicherer, konsolidierter Infrastrukturen lässt sich ein Optimum an Sicherheit erreichen. Dataport hat das noch einmal überprüft. Auch wenn das Unternehmen als Landes- und Kommunaldienstleister formal nicht unter das IT-Sicherheitsgesetz fällt, erfüllt es trotzdem bereits jetzt alle Anforderungen des am 3. Mai 2016 in Kraft getretenen ersten Teils der KRITIS-Verordnung zum IT-Sicherheitsgesetz.

()

Dieser Beitrag ist in der November-Ausgabe von Kommune21 im Schwerpunkt Datenschutz erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit,