Bonn

Isolation statt Detektion

[04.04.2019] Die Stadtverwaltung Bonn sichert mit einer innovativen Lösung von Bromium die Rechner der Mitarbeiter. Der Vorteil: Das Programm schützt beim Surfen und der E-Mail-Kommunikation auch vor bisher unbekannten Schadcodes.

Die Nutzung klassischer Sicherheitstools wie Antiviren-Lösungen, Firewalls oder Web-Filter-Technologien ist in der kommunalen IT – so auch in der Bundesstadt Bonn – heute Standard. Auch Rollen- und Berechtigungskonzepte sind eine Selbstverständlichkeit. Allerdings haben viele Sicherheitsvorfälle gezeigt, dass die Wirksamkeit herkömmlicher Sicherungsmaßnahmen begrenzt ist. Das liegt am technischen Konzept, denn traditionelle Lösungen sind beispielsweise unter Nutzung von Signaturen auf die Malware-Detektion angewiesen. Damit können neue Zero-Day-Attacken, Advanced Persistent Threats oder auch Ransomware-Trojaner kaum zuverlässig aufgespürt werden. Die zunehmenden Attacken mit Ransomware, also Schadprogrammen, die den Computer sperren und nur nach Lösegeldzahlung wieder freigeben, waren auch für die Stadt Bonn der Auslöser, die Erhöhung der Client-Sicherheit in Angriff zu nehmen. Zwei Aspekte waren für die Stadtverwaltung bei der Sicherung der Endgeräte von ausschlaggebender Bedeutung: Sicherheit beim Surfen und Sicherheit bei der E-Mail-Kommunikation.Dabei müssen Kommunen im Unterschied zu vielen Unternehmen zwei Besonderheiten berücksichtigen. Unternehmen können den Empfang von E-Mail-Anhängen oder den Zugriff auf Websites strikt reglementieren, nicht so Kommunen. Mitarbeiter der Verwaltung erhalten Tausende von E-Mails, die nicht ignoriert werden können, da sie berechtigte Bürgeranliegen enthalten können. Ein einfaches Sperren von Websites per Blacklisting ist ebenfalls nicht machbar. Das heißt, Kommunen benötigen Client-Sicherheitslösungen, die einerseits die Zugriffsmöglichkeiten nicht einschränken, andererseits aber auch die Endgeräte und damit das Behördennetz nicht gefährden.

Lösung mit Alleinstellungsmerkmal

Bei der Auswahl einer Client-Sicherheitslösung hat die Stadtverwaltung Bonn zunächst einige Applikationen in Betracht gezogen, welche die Schwachstelle Internet-Browser in den Blick nehmen und ein sicheres Surfen ermöglichen. Allerdings wird mit solchen Lösungen nicht das für die Stadtverwaltung sehr wichtige Thema E-Mail abgedeckt. Auf den Security-Spezialisten Bromium wurde die Stadt Bonn dann durch die Empfehlung einer Landesbehörde aufmerksam. Schnell wurde klar, dass die Bromium-Lösung Secure Platform durch ihr technisches Konzept – Isolation statt Detektion von Schadcode mittels Micro-Virtualisierung – ein Alleinstellungsmerkmal besitzt, sodass auch keine öffentliche Ausschreibung erforderlich war und eine freihändige Vergabe erfolgen konnte. Dirk Schumacher, Leiter Stabsstelle IT-Sicherheit und IT-Strategie im Personal- und Organisationsamt der Bundesstadt Bonn, erklärt: „Bromium bot sowohl technisch die beste, als auch durch das Lizenzierungs- und Wartungsmodell die mittel- und langfristig eindeutig wirtschaftlichste Lösung.“ In einer kurzen Evaluierungsphase im September und Oktober 2017 hat die Stadtverwaltung die Machbarkeit der Einführung der Bromium-Lösung überprüft. Dabei wurden umfangreiche Funktions- und Performance-Tests durchgeführt. Zu berücksichtigen waren rund 4.000 Endgeräte – knapp 1.500 Rechner in der zentralen Verwaltung im Stadthaus, der Rest in den zahlreichen Außenstellen der Stadt. Ein zentrales Testergebnis war, dass etwa ein Viertel aller Rechner nicht die erforderliche Hardware-Ausstattung für einen reibungslosen Einsatz der Bromium-Lösung bot. Folglich wurde ein sukzessiver Roll-out der Secure Platform in Kombination mit der Ablösung älterer

Hardware und der Einführung von Windows 10 als Standardbetriebssystem beschlossen. Bis Ende 2018 waren bereits mehr als 1.000 Geräte mit der Bromium-Lösung ausgestattet. Die Anbindung aller Rechner in Verbindung mit der Windows-10-Implementierung soll Anfang 2020 abgeschlossen sein.

Isolation riskanter Aktivitäten

„Die Bromium-Lösung erlaubte die schnellstmögliche Erhöhung der Sicherheit im Client-Bereich. Schließlich dürfen wir auch bei personell wie budgettechnisch begrenzten Ressourcen keinerlei Abstriche bei der IT-Sicherheit machen“, konstatiert Schumacher. „Wir halten die Bromium-Lösung eindeutig für die derzeit technologisch führende Applikation für die Sicherung von Clients. Unseren Mitarbeitern können wir damit guten Wissens das Motto ‚Keep calm and click on everything’ mit auf den Weg geben.“ Zentrales Charakteristikum der Bromium-Lösung Secure Platform ist, dass nicht die Detektion von Schadcode im Vordergrund steht, sondern das effektive Vermeiden seiner Auswirkungen. Realisiert wird dies durch die Isolierung aller riskanten Anwenderaktivitäten. So besteht Schutz vor Malware, ohne diese als solche erkennen zu müssen. Technisches Merkmal der Bromium-Lösung ist die Hardware-isolierte Micro-Virtualisierung. Tasks werden immer dann in virtuellen Instanzen verarbeitet, wenn es gefährlich werden kann – etwa beim Aufrufen einer Web-Seite, Downloaden eines Dokuments, Öffnen eines E-Mail-Anhangs oder beim Zugriff auf die Daten eines USB-Geräts. Jeder einzelne Task läuft dabei in einer eigenen Micro-VM – und zwar strikt getrennt voneinander sowie getrennt vom eigentlichen Betriebssystem und vom verbundenen Netzwerk. Eine mögliche Schädigung bleibt so immer auf die jeweilige Micro-VM beschränkt, die nach Beendigung einer Aktivität, etwa dem Schließen eines Files, automatisch gelöscht wird. Eine Kompromittierung des Endgeräts und nachfolgend des IT-Netzes ist damit ausgeschlossen.

()

Dieser Beitrag ist in der Ausgabe April 2019 von Kommune21 im Schwerpunkt Datenschutz erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Bonn, Bromium