Ein Sicherheitsportal zur Selbstverwaltung und automatischen Bearbeitung von Sicherheitsvorfällen als Schlüsseltechnologie gegen Masseninfektionen

Jochen Kaiser*, Alexander Vitzthum*, Peter Holleczek*, Falko Dressler†

*Regionales Rechenzentrum †Rechnernetze und Kommunikationssysteme, Institut für Informatik, Universtität Erlangen

Die massive Zunahme von Sicherheitsvorfällen sorgt für eine Verschärfung der Bedrohungslage und eine drastische Zunahme der möglichen bzw. tatsächlichen Schäden. Viele Endsysteme sind mit Malware kompromittiert und bleiben es für lange Zeit, da die Kompromittierung durch den Endnutzer nicht erkannt wird und/oder ohne fremde Hilfe auch nicht entfernt werden kann. Oftmals findet von den betroffenen Systemen aus eine Infizierung/Kompromittierung weiterer Systeme statt. Durch eine frühzeitige Erkennung und Auflösung von Sicherheitsvorfällen kann die Situation deutlich verbessert werden. An der Universität Erlangen wurde die PRISM (Portal for Reporting Incidents and Solution Managment) Plattform entwickelt. Es handelt sich hierbei um ein modulares System, welches Sicherheitsvorfälle über mehrere Pfade gemeldet bekommt und Endnutzern dann die Möglichkeit bietet, diese Sicherheitsvorfälle selbst zu beheben. Dadurch kann fr¡ühzeitig ein Sicherheitsvorfall behoben werden und der Schaden für den Betroffenen und durch frühzeitige Verhinderung der Weiterverbreitung auch für weitere Nutzer begrenzt werden. PRISM liegt eine modulare Architektur zugrunde, welche sich durch einfache Erweiterbarkeit auszeichnet. Die einzelnen Systemkomponenten können dabei folgende Kategorien aufgeteilt werden: Aufzeichnungseinheiten, welche Sicherheitsvorfälle entgegennehmen, zentrale Auswertelogiken, sowie Frontends, wie z.B. ein Selbstbedienungsterminal für die Nutzer-unterstützte Auflösung von Sicherheitsvorfällen. Die Eingabe von Sicherheitsvorfällen kann hierbei auf mehrere Weisen erfolgen. In der experimentellen Implementierung sind Sensoren integriert, die über das IDMEF (Intrusion Detection Message Exchange Format) Protokoll die Sicherheitsmeldungen an den Systemkern weitergeben. Der Datenverkehr eines Nutzers, welcher mit seinem System in das Internet gelangen will, wird dabei auf das Selbstbedienungsterminal umgeleitet. Daher wird bei Nutzung des Web-Browsers der Nutzers nun automatisch auf eine spezielle Seite umgeleitet, welche neben der Darstellung des Sicherheitsproblems auch Zusatzinformationen zur Behebung des Sicherheitsproblems. Ein möglicher Einsatzzweck sind Universitüten, deren offene Forschungsnetze und anspruchsvolle Nutzergruppen besondere Herausforderungen an das IT-Sicherheitsmanagement stellen. Ein anderer Einsatzzweck ist das Management von Endkunden bei Zugangsprovidern. Endkunden sind üblicherweise nicht in der Lage ihr Endsystem so abzusichern, dass keine Sicherheitsvorfälle entstehen. Ebenso werden auch Sicherheitsvorfälle mit Malware nicht erkannt und behoben. Hier kann nun das Sicherheitsportal Abhilfe leisten und den Endkunden kostengnstig auf den Sicherheitsvorfall hinweisen und ihn interaktiv lösen. Die beschriebene Komponente ist Teil einer in der Entwicklung befindlichen Architektur zur Verbesserung der Sicherheit in Netzwerken. Die wesentlichen Eckpunkte der Untersuchung sind hierbei das Einordnen und das Routing bzw. die Eskalation von Sicherheitsvorfällen. Ein weiterer wichtiger Aspekt ist das Finden von Lösungen für diese kritischen Ereignisse. Hierbei wird auch analysiert, wie diese Lösungen in ein Vorfallsmanagementsystem integriert werden können und welche Anforderungen an Schnittstellen hier existieren. Die Untersuchungen sollen dazu beitragen, den massiven automatischen Infektionen mit Malware durch eine möglichst automatisierte Betreuung von Sicherheitsvorfällen zu begegnen. Der Vorteil, welchen Malware durch den Einsatz automatischer Verbreitungsverfahren hat, soll hierbei wieder wettgemacht werden, was eine manuelle Auflösung von Sicherheitsvorfällen nicht leisten kann.