STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Projekt HoneySens

TECHNISCHE
UNIVERSITÄT
DRESDEN

HONEY
SENS

SAX.CERT
Computer Emergency Response
Team des Freistaates Sachsen

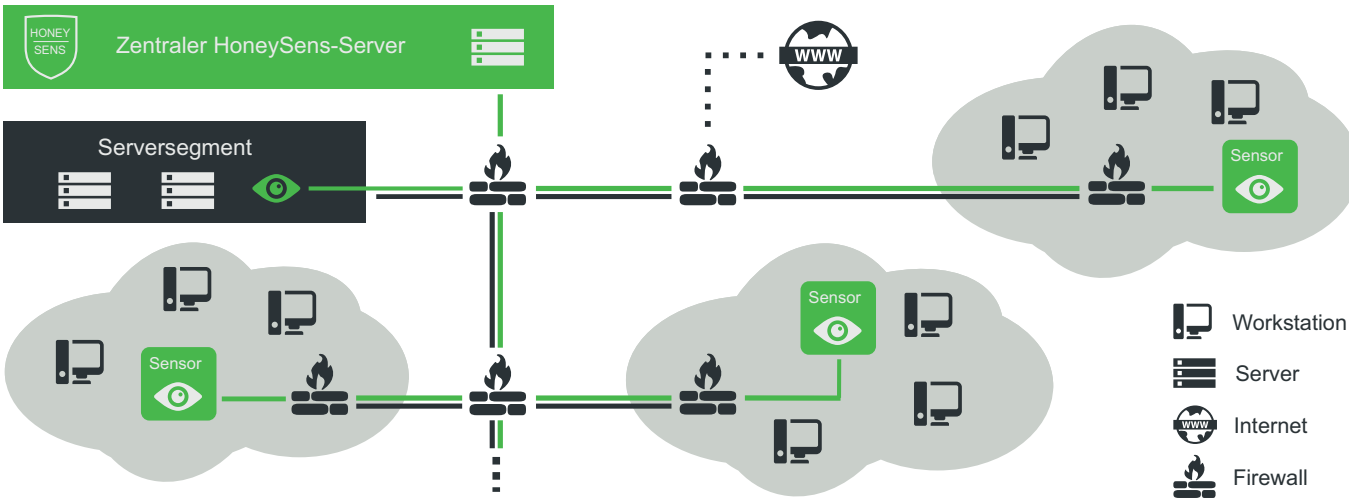
Projekt HoneySens

Die IT-Systeme der Sächsischen Landesverwaltung unterliegen nicht nur Bedrohungen aus dem Internet, sondern können ebenso zum Ziel von Angriffen aus dem internen Netzwerk werden. Ausgangspunkt solcher Angriffe sind typischerweise mit Schadsoftware befallene Rechner. Aber auch unbemerkt in das Netzwerk vorgedrungene Angreifer oder Mitarbeiter, die sich über geltende Sicherheitsbestimmungen hinwegsetzen, stellen Gefahrenquellen dar. Klassische Sicherheitsmaßnahmen, wie zentrale Firewalls und Antivirussysteme, können diese Gefahrenquellen nicht oder nur sehr eingeschränkt ausschalten.

Um auf derartige Gefahren reagieren zu können, wurde vom Beauftragten für Informationssicherheit der Landesverwaltung Sachsen in Zusammenarbeit mit der Professur für Datenschutz und Datensicherheit der Technischen Universität Dresden im Rahmen einer Diplomarbeit das Projekt „HoneySens" entwickelt. Es sieht eine unter Berücksichtigung der Anforderungen des Sächsischen Verwaltungsnetzes (SVN) gestaltete Architektur vor, in der innerhalb gefährdeter Teilnetze platzierte Sensoren Informationen über alle ankommenden verdächtigen Datenpakete aufzeichnen und an eine zentrale Serverkomponente zur Verarbeitung weiterleiten. Administratoren können anschließend mit Hilfe einer komfortablen Web-Anwendung die aggregierten Daten auswerten und bei Bedarf entsprechende Gegenmaßnahmen einleiten.

Automatisierte Erkennung von Angriffen aus dem Inneren

Zur Erkennung potentieller Angriffe kommt auf den Sensoren Honeypot-Software zum Einsatz, deren Zweck die Simulation typischer Netzwerkdienste und zugehöriger Sicherheitslücken ist. Je intensiver ein Eindringling mit diesen „Hackerfallen" kommuniziert, desto mehr Informationen können über dessen Motivation und Vorgehensweise gewonnen werden. Um ein möglichst umfassendes Bild über die Vorgänge innerhalb des Netzwerks zu gewinnen, können die Sensoren auch weitere Datenpakete aufzeichnen. Eine Erkennungsroutine für die von Angreifern häufig zur Informationsgewinnung genutzten Portscans erleichtert zudem die automatische Klassifikation der gesammelten Datenmengen.



Die Architektur des HoneySens-Netzwerks basiert auf einem zentralen Server, der über gesicherte Datenwege (grüne Linien im Bild) von seinen Honeypot-Sensoren Informationen zu verdächtigem Datenverkehr in den überwachten Teilnetzen (Wolkenstrukturen im Bild) erhält und zusammenführt.

Konzeption und Implementierung

Grundanforderungen an das HoneySens-System sind die spezifischen Gegebenheiten des Sächsischen Verwaltungsnetzes und der Wunsch nach einer wartungsarmen, benutzerfreundlichen Lösung. Um die Anforderungen genauer zu spezifizieren, wurde der zu erwartende Datenverkehr in ausgewählen Teilnetzen der Landesverwaltung analysiert. Die dabei gewonnenen Daten waren maßgebend für den Entwurf des autonomen Sensornetzwerks und die Auswahl der eingesetzten Hardwareplattform.

Bei der prototypischen Implementierung des Systems wurde schließlich auf eine hohe Skalierbarkeit durch den Einsatz kostengünstiger Ein-Platinen-Computer als Sensoren, Standardkonformität, leichte Installation und Wartbarkeit, sowie die vollständig verschlüsselte Kommunikation zwischen allen beteiligten Komponenten geachtet.

Ein weiterer wichtiger Teilaspekt war zudem die transparente Integration des Sensornetzwerkes in die derzeit bestehenden Strukturen der Landesverwaltung, um den Betrieb der IT-Infrastruktur nicht zu beeinträchtigten.

Effiziente Abläufe

Damit auch nicht im Bereich der Informationssicherheit geschulte Administratoren mit dem HoneySens-System arbeiten können, wurde bei der Entwicklung des Prototyps viel Wert auf eine leicht verständliche graphische Benutzeroberfläche gelegt. Die Web-Anwendung unterstützt deshalb die Benutzer sowohl bei allen anfallenden Arbeitsschritten, darunter die komfortable Integration zusätzlicher Sensoren und die Bereitstellung automatischer Updates der Sensor-Software, als auch bei der Auswertung aller gesammelten Daten.

Eine flexible Benutzerverwaltung stellt zudem sicher, dass nur berechtigte Personen Zugang zum System besitzen. Techniken des „Responsive Web Design" garantieren ferner, dass die Benutzerschnittstelle auch auf Mobilgeräten wie Smartphones und Tablets ohne Einschränkungen genutzt werden kann.

Auch bei der Konzeption der zentralen Serverkomponente wurden Möglichkeiten zur unkomplizierten Installation berücksichtigt: Die Bereitstellung der Software in Form von virtualisierbaren Containern assistiert beim flexiblen, transparenten Betrieb der Anwendung und vereinfacht zukünftige Updates.

Geplante Weiterentwicklung

Die prototypische HoneySens-Implementierung wurde im Rahmen der Diplomarbeit in einem mehrwöchigen Testzeitraum innerhalb des Sächsischen Verwaltungsnetzwerkes und in einem Teilnetz der TU Dresden erprobt und verbessert.

In einem nächsten Schritt wollen die Kooperationspartner den vorliegenden Prototyp für den Einsatz in komplexen Netzstrukturen weiterentwickeln und dabei auch weitere potentielle Anwender einbinden. Hauptaugenmerk ist dabei die Untersuchung und Bewertung der vielfältigen Anforderungen, die sich aus dem Einsatz innerhalb eines Verbunds aus zahlreichen heterogenen Teilnetzen ergeben.

Abschließend sollen die gewonnenen Erkenntnisse über sinnvolle Gestaltungs- und Anwendungsmöglichkeiten eines solchen Sensornetzwerks nicht nur für die Erhöhung der Informationssicherheit in Sachsen genutzt, sondern auch in die entsprechenden Gremien der Länder und des Bundes eingebracht werden.

Wollen Sie mehr über das Projekt HoneySens erfahren, wenden Sie sich bitte an:

Sächsisches Staatsministerium des Innern
Beauftragter für Informationssicherheit des Landes
Wilhelm-Buck-Straße 4, 01097 Dresden
E-Mail: bfis-land@smi.sachsen.de

Dipl.-Inf. Pascal Brückner
E-Mail: pascal.brueckner@sylence.cc

Herausgeber:
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 2
01097 Dresden

Redaktion:
Referat 65 „Informationssicherheit in der Landesverwaltung, Cybersicherheit"

Gestaltung, Satz und Motive:
Haus E, Chemnitz; [2012], Bigstock
Staatsbetrieb Sächsische Informatik Dienste (SID) 2014

Druck:
Flyeralarm GmbH

Redaktionsschluss:
Dezember 2015

Verteilerhinweis:
Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von politischen Parteien noch von deren Kandidaten oder Helfern zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.