Technische Berufsschule Zürich TBZ
Höhere Fachschule
Sihlquai 101
8090 Zürich

Advanced Malware Protection

Diplomand: Fabian Kälin
Klasse: ITSE14b
Schulexperte: Hansrudolf Kramer
Firmenexperte: Frank Hauser
Firma: UniversitätsSpital Zürich

Fabian Kälin

UniversitätsSpital Zürich

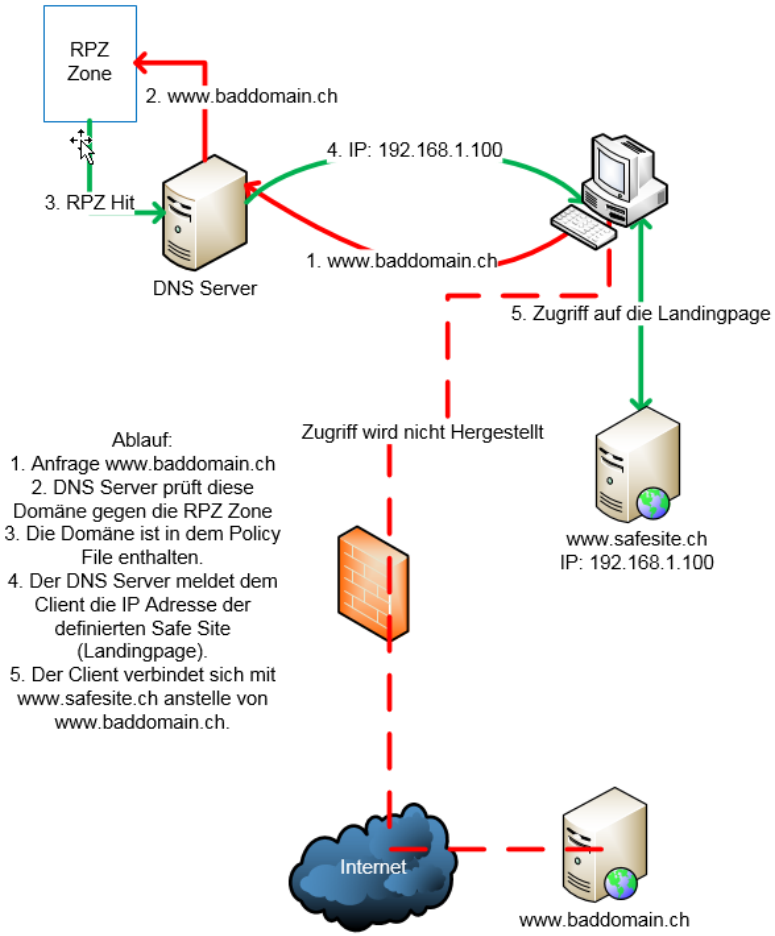
Ausgangslage

Die am UniversitätsSpital Zürich eingesetzten Sicherheitssysteme im Perimeter blockieren musterbasiert aktuell ca. 200 verdächtige Programme pro Monat und schützen dabei Clients und Server beim Zugriff ins Internet. Zusätzliche Schutzeinrichtungen auf den Endpoints ergänzen die Überwachung, resp. Erkennung und Bereinigung von potenziell schadhafter Software. In regelmässigen Abständen werden diese Systeme mit neuen Erkennungsinformationen ergänzt.

Allerdings finden sich im Spitalumfeld Systeme, welche heute nur teilweise von diesen Schutzmassnahmen profitieren können. Zum Beispiel dürfen bei gewissen Geräten keine Updates installiert oder Schutzeinrichtungen konfiguriert werden, ohne die Zusage der Hersteller. Diese Systeme basieren auf unterschiedlichen Betriebssystemen und sind nicht Teil der sonst standardisierten und zeitnah aktualisierten IT-Infrastruktur. Dadurch entsteht ein erhöhtes Risiko für eine mögliche Infektion, resp. die Erkennungsrate einer Infektion sinkt, weil die Integration in die bestehenden Schutz- und Erkennungsmassnahmen (Monitoring) fehlt.

Im Rahmen dieses Projekts wird eine Lösung verfolgt, welche die bisherige Schutzinfrastruktur ergänzt. Sie soll für die standardisierte IT-Infrastruktur sowie für alle anderen Geräte

Technische Berufsschule Zürich TBZ
Höhere Fachschule
Sihlquai 101
8090 Zürich



wirksam sein und mögliche Infektionen verhindern, resp. erkennen können.

Einführung Malware

Im Rahmen der Diplomarbeit wurde zu Beginn der Arbeit ein Dokument über Malware Typen und deren Verhaltensweisen erfasst. Dadurch wurde als Gemeinsamkeit der meisten Malware Typen die Kommunikation mit "Command & Control Servern" festgestellt. Diese wird in vielen Fällen über Domain Namen geführt. Grund dafür ist, dass die "Angreifer" die Server flexibel ansteuern können. Das heisst, es muss nur die hinterlegte IP Adresse angepasst werden. Anderen falls müssten sie die Malware mit der neuen IP Adresse erneut verteilen.

Hauptstudie

Im Rahmen der Hauptstudie wurden zwei Produkte näher angeschaut. Als erstes System war ist dies ein PassiveDNS, welches alle DNS abfragen, die aus dem USZ getätigt werden, im Hintergrund aufzeichnet. Als zweites System wurde eine DNS Firewall angeschaut. Dies sind DNS Zonen, welche auf dem Resolver abgearbeitet werden. Diese bieten die Möglichkeit, gewisse Domänen nicht aufzulösen, sondern auf eine Landingpage weiterzuleiten. Es sollte zusätzlich eine Log Korrelation erarbeitet werden, damit die Identifikation des anfragenden Clients vereinfacht wird.

Realisation

Das PassiveDNS System und die DNS Firewall wurden ins USZ Netzwerk eingebunden. Durch das Aufzeichnen und Blockieren der DNS anfragen besteht nun die Möglichkeit, unsere gesamte Infrastruktur zu schützen. Es werden alle DNS Anfragen sämtlicher Endgeräte in unserem Netzwerk, ohne Änderungen an ihrer Konfiguration, überwacht und geschützt. Für die Erkennung wurde von der Firma SWITCH die RPZ (Response Policy Zonen) Konfiguration gemietet. Damit erhalten wir sowohl die von der SWITCH als auch die von SURBL gepflegten Zonen. Es wurde ein Web Server im USZ aufgeschaltet und eine Blockpage eingerichtet.