Automatic Firewall Pinholing Process

KURZZEICHEN	BIT-FW-Pinhole
AUFTRAGGEBER/IN	Fritz Weyermann, Bundesamt für Informatik und Telekommunikation
STUDENT/IN	Marco Gauch
DOZENT/IN	Michael Mäder, Rudolf Scheurer
EXPERTE/EXPERTIN	Daniel Brügger, Bundesamt für Landestopografie swisstopo
Nr.	B20T05
TYP	Bachelorarbeit
KONTAKT	marco.gauch@edu.hefr.ch; gauchmarco@gmail.com

Im Rahmen der Bachelorarbeit wird das Mandat «*Automatic Firewall Pinholing Process*» vom Bundesamt für Informatik und Telekommunikation (BIT) übernommen und bearbeitet. Die Bachelorarbeit baut auf dem soliden Fundament des Semesterprojektes 6 auf.

Das Mandat forderte die Digitalisierung und Automatisierung eines administrativen und zeitaufwendigen Prozesses. Konkret geht es um die Behandlung der Anträge zur Öffnung/Schliessung von Firewall-Ports und die Provisionierung der Firewall-Regeln.

Aktuell erfolgt die Antragsstellung (Abb 1) einer Öffnung/Schliessung über eine Wordvorlage und erfordert die Interaktion von mindestens vier verschiedenen Akteuren.

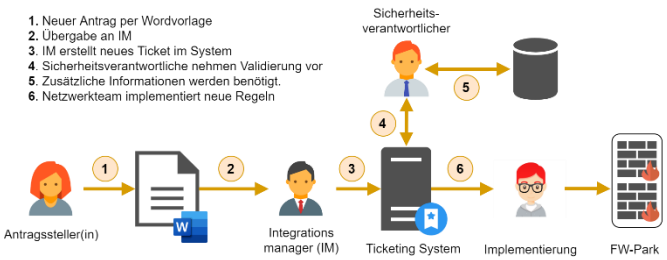

Abb 1: Antragsstellung und Provisionierung, IST

Erledigte Arbeiten

Im vorgängigen Semesterprojekt wurde bereits eine Webapplikation entwickelt, welche die Antragsstellung neu über ein Web-Formular erlaubt. Ein Validierungsmechanismus ermöglicht den Sicherheitsverantwortlichen die Anträge direkt über die Webapplikation zu validieren.

In der Bachelorarbeit wurden zusätzliche Funktionen für die Webapplikation implementiert. Das Hauptaugenmerk wurde hier auf die automatische Provisionierung der Firewall-Regeln gelegt. Anhand gezielter Kriterien wurde die *AlgoSec Security Management Suite* (ASMS), eine Softwarelösung für die automatische Provisionierung von Firewall-Regeln, ausgewählt und eingesetzt.

In einer Testumgebung, wurden drei Firewalls, drei Clients und ein Router virtualisiert. Nebst dem produktiven Netz wurde ein Management-Netzwerk geplant, welches den Informationsaustausch zwischen AlgoSec und den Firewalls gestattet.

Validierung eines Antrages

Damit den Sicherheitsverantwortlichen der Validierungsentscheid erleichtert wird, wird im Hintergrund eine Simulation für den angeforderten Datenverkehr gestartet. Während der Validierung wird für jeden Eintrag der Status und ein Link zur Simulation angezeigt (Abb 2).

Port #	TCP/UDP	Tech. comment	ALLOW/DROP	AlgoSec Status	Trafic Simulation
5500	TCP	tcp/5500	ALLOW	✗	AlgoSec Link
5700	TCP	tcp/5700	ALLOW	✗	AlgoSec Link
7777	TCP	tcp/7777	ALLOW	✓	AlgoSec Link
65000	TCP	tcp/65000	ALLOW	✓	AlgoSec Link

Abb 2: Validierung Antrag mit vier Portöffnungen

Der «*AlgoSec Link*» führt direkt zur Simulation, welche die betroffenen Firewalls grafisch hervorhebt. Des Weiteren werden die dazugehörigen Regeln identifiziert, welche den Datenverkehr blockieren oder erlauben.

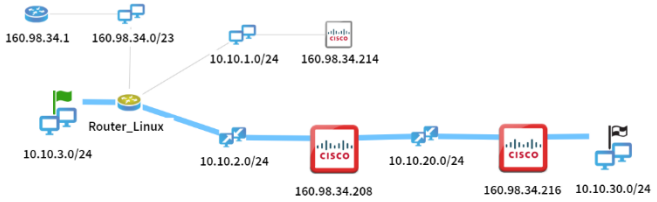

Abb 3: Simulation des Datenverkehrs, Status BLOCKED

Mithilfe der Simulation des Datenverkehrs (Abb 3) verschafft sich der Sicherheitsverantwortliche den notwendigen Überblick über die Netzwerktopologie und ermöglicht so einen beschleunigten Validierungsentscheid.

Automatische Provisionierung

Im Rahmen der Bachelorarbeit wurden die Automatisierungsstufen *manuell, semi-automatisch* und *automatisch* definiert. Dank der stetigen Weiterentwicklung der Webapplikation und der Integration der AlgoSec API, konnte die automatisierte Provisionierung erreicht werden. Mit Validierung durch den Sicherheitsverantwortlichen wird per API ein Ticket in der ASMS erstellt. Insofern kein Risiko besteht und keine Schliessung beantragt wurde, lässt sich das Ticket automatisch abhandeln. Das heisst die Firewall-Regeln werden auf den entsprechenden Firewalls aktiviert. Eine Interaktion durch den Sicherheitsverantwortlichen ist nicht erforderlich. Anhand einer weiteren Simulation des beantragten Datenverkehrs (Abb 4) wird gezeigt, dass die Öffnung korrekt umgesetzt wurde.

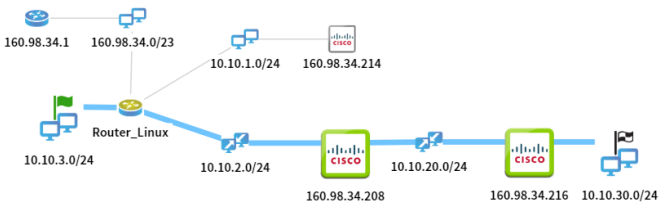

Abb 4: Simulation des Datenverkehrs, Status ALLOWED

Fazit

Im Rahmen der Bachelorarbeit sowie dem Semesterprojekt 6 konnte die Antragsstellung einer Port-Öffnung/Schliessung und deren Provisionierung erfolgreich digitalisiert und automatisiert werden. Der optimierte Prozess wird in Abb 5 dargestellt. Vergleicht man den optimierten Zustand mit Abb 1, wird ersichtlich, dass die Anzahl Akteure reduziert und die Durchlaufzeit verkürzt werden konnte. Mit dem erarbeiteten Prototyp und der Testumgebung konnten erfolgreich alle geforderten Ziele umgesetzt werden.

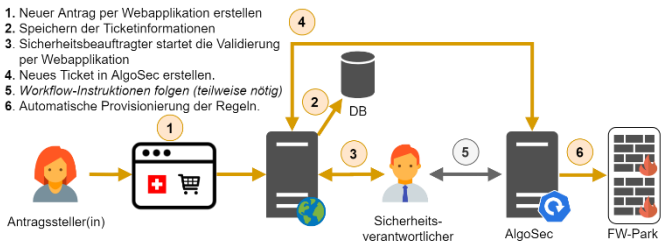

Abb 5: Optimierte Antragsstellung und Provisionierung