Paradigmenwechsel in der IT Security

Um den Angriffs-Schutz von KMU-Netzwerken stark zu erhöhen, entwickelte Felix Hosner den Lösungsansatz einer Monolithischen Client/Server Architektur. Die Arbeit verfasste er im Rahmen seiner Master Thesis unter der Ägide von Prof. Rolf Lanz

Mit den gebräuchlichen Sicherheitsmassnahmen (Patching, Antivirus, Firewall und Benutzerschulung) konnten früher IT-Bedrohungen klein gehalten und das Schadenspotential minimiert werden. Heute, in der Zeit professioneller Attacken genügt dieser Schutz bei weitem nicht mehr. Netzwerke sind hohen Angriffsrisiken ausgesetzt, was aktuelle und brisante Fälle der letzten Jahre belegen. Die IT-Gefahren haben sich geändert, aber das klassische IT-Sicherheitsdispositiv ist immer noch das Gleiche. Die IT-Organisation stösst hier an ihre Grenzen. Neue Konzepte sind gefragt.

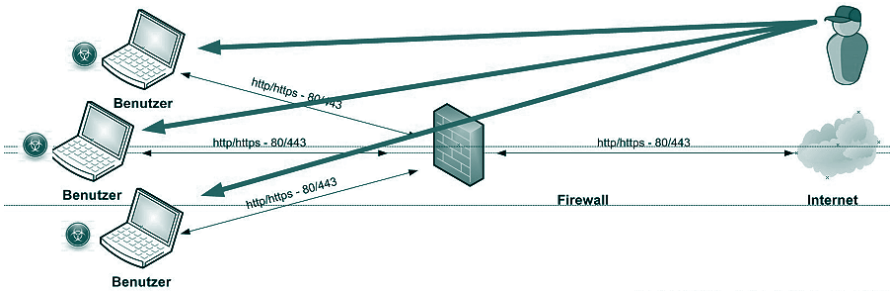
Verteidigungsoptionen im Cyberwar

Es gibt keine Alternativen zur existierenden Internettechnologie. Und da heute diese Technologie nicht nur im Internet verwendet wird, sondern weit in die Firmennetzwerkarchitektur integriert ist, enden die Probleme nicht an der Haustüre (Firewall), sie dringen bis ins Herz der Informatik-Landschaft ein. Wie aber ist derartigen Übergriffen zu begegnen? Bislang fehlte diesbezüglich ein systematisches Konzept. Einfach den Internetstecker zu ziehen und den Router auszuschalten würde zum Zusammenbruch des jetzigen Wirtschaftssystems führen. Doch, welche andere Optionen gibt es, um KMU-Netzwerke in Anbetracht der realen Gefahren angriffsresistenter und betriebssicherer zu machen? Dieser Frage geht die vorliegende Master Thesis nach.

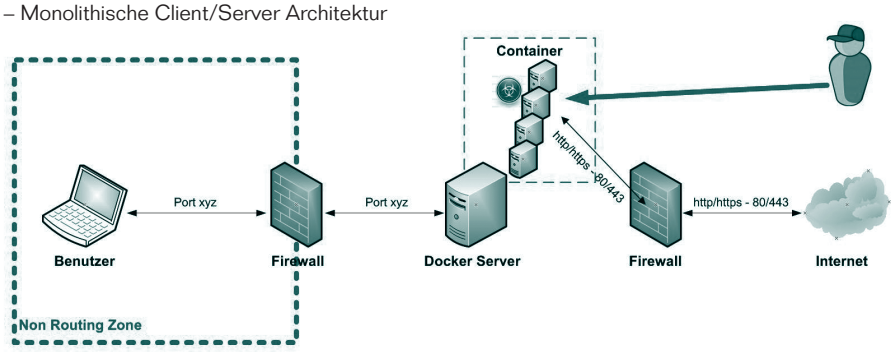
Unterbindung des direkten Datenaustauschs

Die ausgewählte Option einer Monolithischen Client/Server Architektur ermöglicht es, zentrale Elemente der IT-Infrastruktur vom Internet zu trennen – ohne von ihm abgeschnitten zu sein. Sie verfolgt den Ansatz, die Visibilität der Systeme zu reduzieren. Ihre Grundidee besteht in der Abkopplung der zentralen Systeme von der direkten Internetkommunikation. So genannte «Non Routing Zonen» verunmöglichen es dem Netzwerk, direkt mit einem Nachbarnetz zu kommunizieren – auch mit dem «Nachbarnetzwerk» Internet. Die Zone ist abgeschottet und kann vom Internet nicht erreicht werden. Ihr Wirkungsbereich wird individuell definiert und umfasst idealerweise die Kernsysteme und deren Clients.

Ausgangslage – Monolithische Client/Server Architektur



Docker Lösung – Monolithische Client/Server Architektur



Terminal Server und Gateway als Lösungsansatz

Den Datenaustausch zwischen der monolithischen «Non Routing Zone» mit dem Internet gewährleistet ein Terminal Server. Er verfügt über zwei Schnittstellen: eine, die intern mit den Clients kommuniziert und eine zweite in ein Routing-Netzwerk mit Internetanbindung. Der Client verbindet sich per RDP-Protokoll auf den Terminal Server. Dieser stellt die Verbindung ins Internet her und bietet dem Client entsprechende Browser-Funktionalitäten an. So können weiterhin Remote Support Tools eingesetzt und Home Office-Arbeitsplätze vernetzt werden.

Fazit – das Konzept kann die Sicherheit stark erhöhen

Mit der vorliegenden Master Thesis über eine Monolithische Client/Server Architektur ist eine wesentliche Vorarbeit für ein Sicherheitskonzept geleistet, das einen Paradigmenwechsel in der IT Security von KMU-Netzwerken einläuten könnte. Das Konzept zeigt auf, wie die Angriffsfläche mit verhältnismässig geringem Aufwand auf wenige Systeme reduziert werden kann. Ein überwachter und dokumentierter Datenaustausch via Gateway ist eine gute Grundlage für eine effektive «Data Leakage Prevention» intern und extern. Für die Weiterentwicklung und Umsetzung in die Praxis werden sich Herausforderungen der Automatisierung und Individualisierung stellen. Vorstellbar ist ein «Out of the box feature» für KMU-Betriebe, die sich ihrer IT-Security-Problematik bewusst sind.

Eckdaten zur Master Thesis Monolithische Client/Server Architektur

FRAGESTELLUNG: Wie können KMU-Netzwerke kostengünstig geschützt werden?
PROBLEMATIK: Direkter Datenaustausch im Internet
ANFORDERUNG: Angriffsflächen reduzieren, Datenaustausch kontrollieren
LÖSUNGSANSATZ: Monolithische Client/Server Architektur
UMSETZUNG: Möglich nach Evaluation von Marktbedürfnis und Entwicklungspotenzial
DER AUTOR: Felix Hosner, Aspirant MAS N&S; Berner Fachhochschule, Technik und Informatik Softwareschule Schweiz

COMPUTER COACH GmbH

Interview mit Felix Hosner

Monolithische Client/Server Architektur für maximierte IT Security

Sie begründen in Ihrer Masterarbeit im Bereich Information Technology Networking & Security der Berner Fachhochschule den Vorschlag, künftig Monolitische Client/Server Architekturen einzusetzen. Warum?

KMU Netzwerke sind stark bedroht. Die Angriffe auf Netzwerkinfrastrukturen haben in den letzten Jahren an Qualität zugenommen – intern und extern. Firewalls, Patches und Virentools leisten gegenüber den neuen Angriffsmöglichkeiten kaum noch genügend Schutz. Das Konzept der Monolitischen Client/Server Architektur kann dafür Abhilfe schaffen.

Wie kann die Sicherheit erhöht und gewährleistet werden?

Es wird eine monolithische «Non Routing Zone» geschaffen in der die Kernsysteme und Benutzer/Clients vom direkten Internet-Zugang abgeschnitten sind. Der Datenaustausch mit dem Internet wird allein durch ein Terminal Server Gateway sichergestellt. Dabei findet ein Protokollwandel statt von http/https-Text-Daten in einen RDP-Bild-Strom, wodurch die angreifbare Fläche auf nutzbare Daten für Hacker praktisch auf Null reduziert wird.

Was ist der Unterschied und wo liegen die konkreten Vorteile?

In einer «Routing Zone» ist für Hacker der Zugriff auf die effektiven Daten jedes Client durch die Umgehung der Firewall problemlos möglich. In der «Non Routing Zone», in der ausschliesslich der Terminal Server mit den Clients eine interne Verbindung hat, ist das Eindringen via Internet kaum möglich. Zudem kann auch der interne Datenaustausch gezielt überwacht und die Aktivitäten aufgezeichnet werden. Der hauptsächliche Vorteil ist der wirkungsvolle Schutz des eigenen IT-Systems vor Angriffen aus dem Internet. Denn erst durch die Entkopplung der IT vom Internet können die Schutzmassnahmen wie Firewalls, Patches und Virentools ihren Zweck gegenüber Bedrohungen auch tatsächlich erfüllen.

Wo liegen die Herausforderungen bei der Umsetzung?

Der Ansatz der Monolitischen Client/Server Architektur muss weiterentwickelt werden. Primär der Aufbau, die Dokumentation und die Analyse der Netzwerkinfrastruktur, der RDP-Services und des Datenaustausch-Gateways. Zudem müssen Lösungen erarbeitet werden für die Wartungsschnittstellen, die Überwachung und für persönliche BYoD-Systeme. Sekundär sind auch Aspekte wie Skalierung, Outsourcing, Appliance-Lösungen und Risikoanalysen zu lösen.

Die Master Thesis von Felix Hosner: Monolithische Client/Server Architektur ist an der Berner Fachhochschule Technik und Informatik – Softwareschule Schweiz einsehbar (MT–FS14.9)

Der Kontakt

Computer Coach GmbH

Thalgutstrasse 10 | CH–3116 Kirchdorf BE | T +41 (0)31 782 12 00 | F +41 (0)31 782 12 02

felix.hosner@computer-coach.ch