Informationsblatt Resilienzanalyse mit securiCAD®

Im 21. Jahrhundert ist der Schutz der Informationen und des Unternehmens-Wissens elementarer Erfolgsbestandteil. Der Schutz dieser vor unberechtigten Blicken und Angreifern aus dem Internet ist eine wichtige Aufgabe jedes Unternehmens. Doch die richtigen Maßnahmen zu finden, ist dabei nicht immer einfach.

Die Resilienz beschreibt die Widerstandsfähigkeit eines IT-Systems bzw. der darin gespeicherten Daten. Dabei wird betrachtet, welche Angriffswege möglich sind. Aus diesem Wissen lassen sich strategische Entscheidungen für den bestmöglichen Schutz von Wissen und Daten ableiten.

Resilienter werden

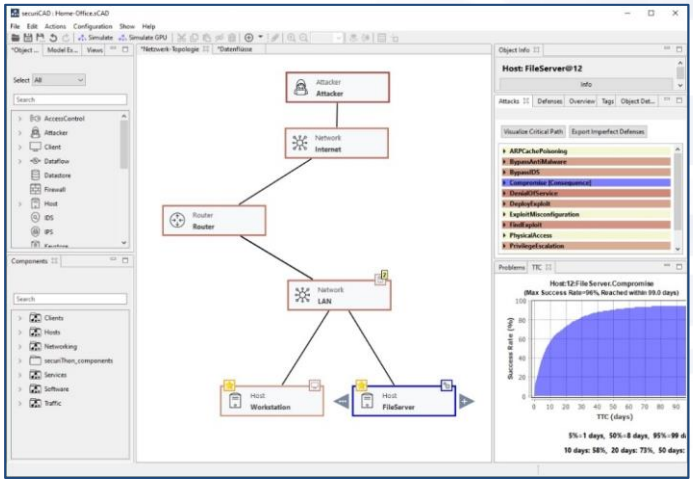
Der erste Schritt zur Resilienzsteigerung ist die **Modellierung** der Infrastruktur zur Identifikation von Schwachstellen. Hierzu entsteht in securiCAD® ein digitaler Zwilling der System-Landschaft. Innerhalb dieses Zwillings findet die **Angriffs-Simulation** statt. Diese gibt Aufschluss über die potentiellen Angriffswege und damit den Reifegrad der Infrastruktur-Verteidigung.

Die Software
- Modellieren
- Simulieren
- Analysieren
- Vergleichen

Die Beratung
- Modellierung
- Szenario-Entwicklung
- Schwachstellen-Analyse
- Maßnahmen priorisieren

Modellieren

securiCAD® professional ist in der Lage die strukturellen Zusammenhänge der Systemlandschaft abzubilden. Hierfür werden sogenannte Assets genutzt, welche eine Facette der Umgebung repräsentieren. Mit den Einflussgrößen Angriffspotential und Verteidigungsmechanismen wird beschrieben, wie die Systemlandschaft agiert.



Durch die Verknüpfung der Assets entsteht ein zusammenhängendes Bild der Infrastruktur bzw. des Infrastruktur-Teils, welches betrachtet wird.

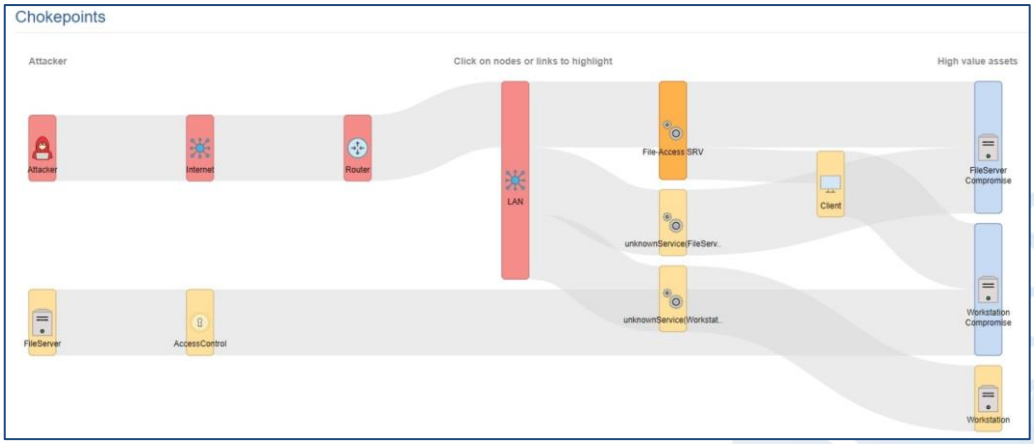
Dabei wurden verschiedene Derivats-Sprachen für verschiedene System-Umgebungen entwickelt, um Informations-Technologie (Büro-IT), Operational-Technologie (Industrie) und Rechenzentrums-IT (Cloud-IT) auf einem gemeinsamen Nenner zu betrachten.

Simulieren

Die Angriffs-Simulation, welche securiCAD® durchführt, basiert auf den Forschungs-Ergebnissen der Königlich Technischen Hochschule (KTH) in Stockholm, welche in über 10 Jahren Forschung den Ansatz zur Resilienz-Analyse auf Basis quantitativer Stochastik geschaffen hat.
securiCAD® profitiert von diesen Erkenntnissen und wird stetig weiterentwickelt und mit neuen Angriffsmustern versehen, sodass die Analyse immer auf dem aktuellsten Stand durchgeführt wird.
Die Simulation überprüft, welche technischen Wege zwischen einem potentiellen Angreifer und der Kronjuwelen der Systemlandschaft möglich sind. Dabei wird überprüft, wie wahrscheinlich es ist, dass ein Angreifer zum Erfolg kommt. Ebenso wird die Infrastruktur auf strukturelle Schwächen hin untersucht.

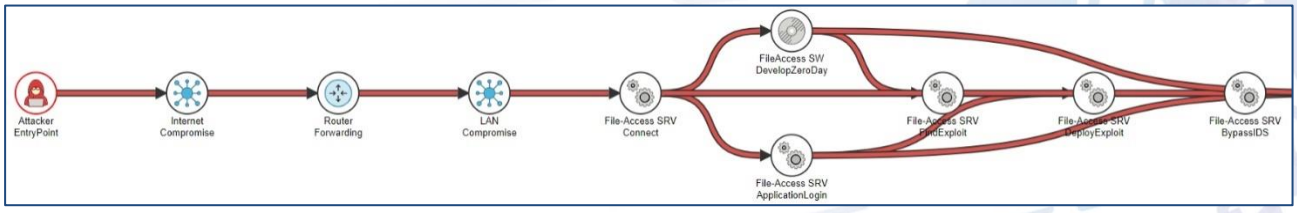
Analysieren

Potentiell kritische Wege in die Systemlandschaft, basierend auf den aktuellsten Angriffsmethoden, werden priorisiert und visualisiert. Dabei illustrieren die Engstellen der Infrastruktur, die Facetten, welche eine maßgebliche Rolle bei Angriffen auf Kronjuwelen spielen.



Mit Hilfe dieser Informationen lassen sich strukturelle Schwachstellen oder Hot-Spots in der Systemlandschaft erkennen und zukünftig bestmöglich überwachen, um die Erfolgschance der Angreifer zu minimieren.

Ein genauerer Blick zeigt außerdem, welche alternativen Wege bzw. Abhängigkeiten es für bestimmte Angriffe gibt. Somit lassen sich Infrastruktur-Zusammenhänge direkt aus Angreifer-Perspektive betrachten.



Vergleichen

securiCAD® errechnet einen Resilienzwert auf Basis der Angriffssimulation. Dabei werden potentiell mögliche Angriffe, die dagegenstehende Verteidigungs-Struktur sowie die Vernetzung zur Bestimmung berücksichtigt.

Im Ergebnis lassen sich die aktuelle Lage mit identifizierten Maßnahmen zur Absicherung der Systemlandschaft in Relation zu einander setzen. Erklärtes Ziel ist es dabei, die strategischen Maßnahmen zu forcieren, die einen langfristig sicheren Betrieb ermöglichen.

Aus der Analyse können sich sinnvolle Änderungen an der Systeminfrastruktur ergeben. Diese werden in alternativen Szenarien beschrieben. Dabei wird geprüft, welche Auswirkungen Änderungen der Infrastruktur auf die Systeme und den Resilienzwert haben. In dieser Plan-Simulation können Änderungen, Einführung neuer Systeme aber auch Rückbau von Alt-Systemen gleichermaßen betrachtet werden.

Risks

Each column contains a summary for all high value assets of a selected simulation. The high value assets are grouped by object type. Click on the object types to see details for each object type

	IST-Zustand	System-Härtung	Neue Firewall
Host			
Workstation.Compromise			
Time to compromise	12 day(s)	52 day(s)	N/A
Consequence	3	3	3
Probability	0.85	0.61	0.21
Risk	High	Medium	Low
FileServer.Compromise			
Time to compromise	7 day(s)	29 day(s)	N/A
Consequence	10	10	10
Probability	0.95	0.68	0.23
Risk	Critical	Critical	High

Die Geschichte hinter dem Ansatz

Die Erarbeitung des Ansatzes sowie die Überführung in ein langfristig gepflegte Software-Produkt, stammen aus der Motivation der Europäischen Union, einen objektiven Messwert zur Beschreibung von Informations-Sicherheit zu entwickeln.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 673980.

Die Entwicklung von securiCAD® wurde von der EU im Rahmen des Horizon 2020 Programmes als herausragende Technologie gefördert.

CYBEResilienz implementiert und berät

Die CYBEResilienz GmbH Berater sind zertifiziert durch den Hersteller foreseeti. Sie übernehmen damit auf Wunsch alle Aufgaben im Resilienz-Projekt, von der Modellierung bis hin zur Dokumentation.