THINK SAFE THINK ICS

industrial engineering

Risikoanalyse mit securiCAD®

Schützen Sie Ihr wertvollstes Gut

Informationen sind die Währung des 21. Jahrhunderts. Der Schutz von Informationen ist eine der wichtigsten Aufgaben der heutigen global vernetzten Gesellschaft. Speziell jene Netze, deren Ausfall katastrophale Folgen hätte – die sogenannten kritischen Infrastrukturen – müssen auf höchstem Niveau geschützt werden. Aufgrund dieses hohen Gefährdungspotenzials müssen Maßnahmen zur Risikoanalyse von Netzwerken ganzheitlich greifen. Hier hilft securiCAD®!

Schwachstellen erkennen & eliminieren

Mit securiCAD® haben Sie die Möglichkeit, Ihre Risiko-Betrachtung auf das nächste Level zu bringen. Nutzen Sie die Vorteile der Software und profitieren Sie von den Erfahrungen der ICS-Mitarbeiter.

Die Software: securiCAD®
- Abbildung des Netzwerkes
- Simulieren von Angriffen
- Identifizieren von Schwachstellen
- Durchführung von Vorher-Nachher-Vergleichen

Das Know-how: ICS GmbH
- Modellieren des Netzwerkes
- Konzeptionieren von Szenarien
- Analysieren der Schwachstellen
- Entwickeln und Bewerten von Maßnahmen

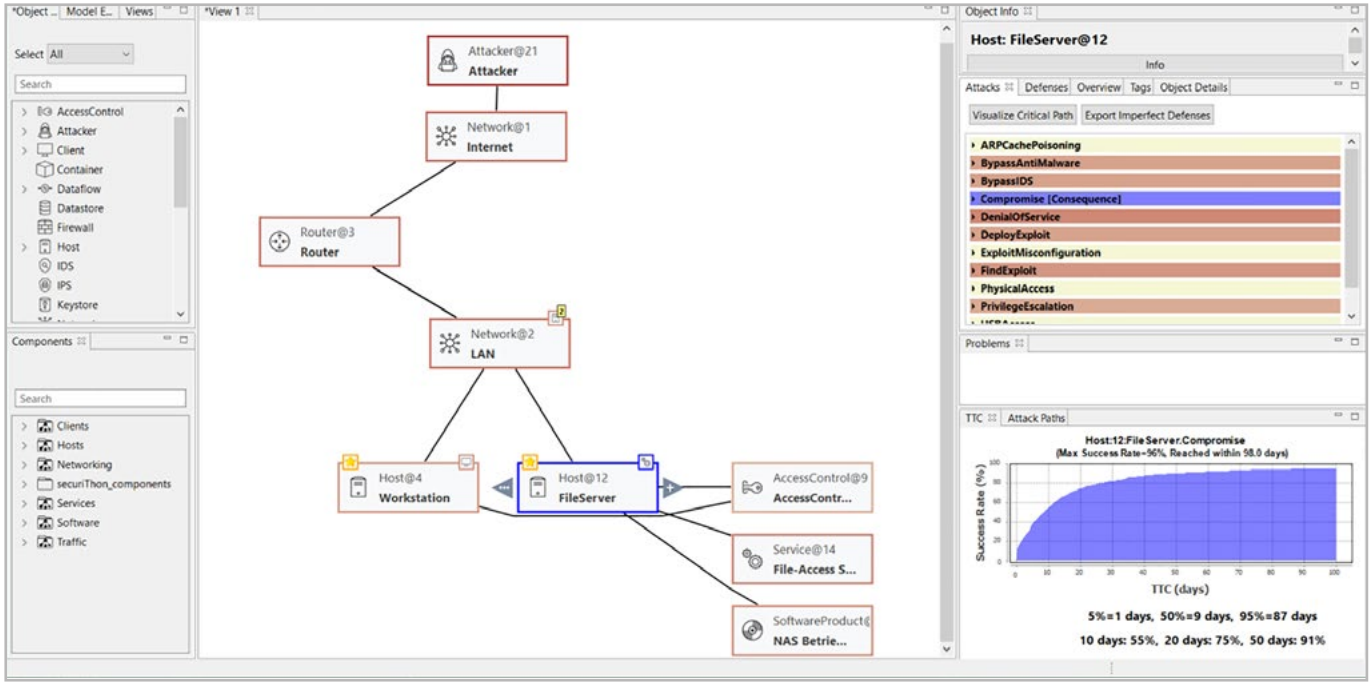
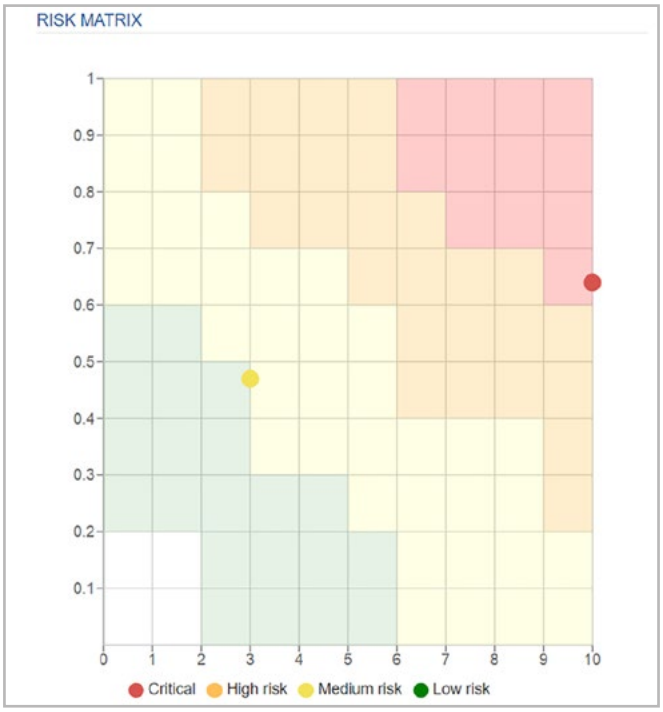
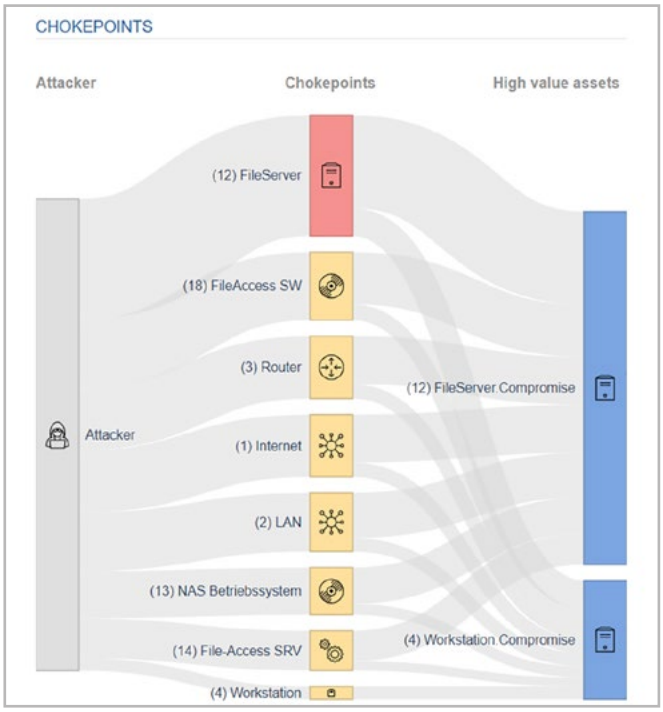


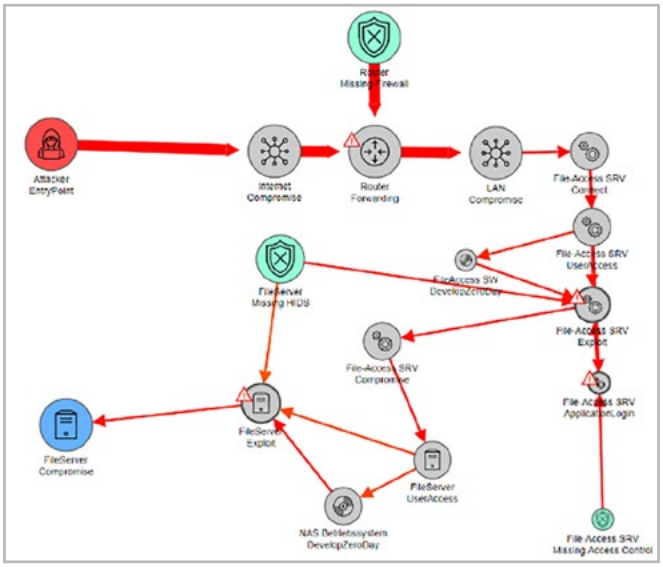
Abbildung 1 securiCAD® simuliert Angriffe und analysiert Schwachstellen



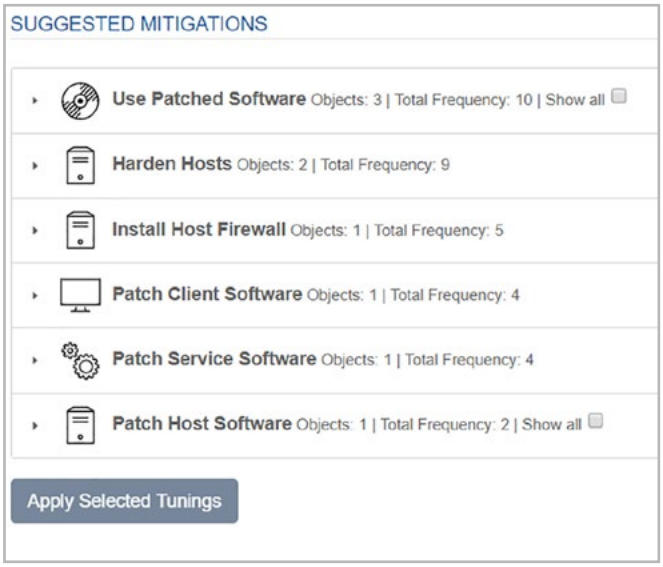
securiCAD® misst die Korrumpierungswahrscheinlichkeit des jeweiligen Assets. Dabei liefert eine Risiko-Matrix einen Überblick darüber, welche Systeme welchem Risiko ausgesetzt sind (Y-Achse) und wie wichtig diese Systeme für die Infrastruktur sind (X- Achse), um eine erste Priorisierung abzuleiten.



securiCAD® errechnet die Wahrscheinlichkeit der Angriffswege und die Beteiligung der verschiedenen Infrastruktur-Assets. Somit lassen sich gemeinsame Nenner ableiten und die Infrastruktur-Maßnahmen gemäß den beteiligten Systemen und des System-Risikos priorisiert umsetzen.



Aus der Simulation und den abgeleiteten Wahrscheinlichkeiten wird der wahrscheinlichste Angriffspfad bestimmt, sodass der Fokus darauf gelegt werden kann, diesen Angriffspfad möglichst schwierig zu gestalten.



Die abgeleiteten Maßnahmen können in seperaten Modellen betrachtet werden. Dabei ist es möglich Extrem-Szenarien anzunehmen oder das aktuelle Patch-Niveau moderat zu verbessern.

Die verschiedenen Simulationen lassen sich gegenüberstellen, um eine Entscheidungsvorlage auf Basis von Kosten und Nutzen - für die IT-Security - zu erstellen. Somit lassen sich objektiv Entscheidungen auf Basis von Zahlen, Daten, Fakten herstellen und diese Investitionen auch später noch begründen. Kaufentscheidungen auf Basis von technischen Diskussionen gehören damit der Vergangenheit an.

	Initial simulation Feb 11 2019, 12:46	AV+PW-Policy Feb 11 2019, 12:47
Host		
FileServer.Compromise		
Time to compromise	8 day(s)	23 day(s)
Consequence	10	10
Probability	0.84	0.64
Risk	Critical	Critical
Workstation.Compromise		
Time to compromise	12 day(s)	50 day(s)
Consequence	3	3
Probability	0.74	0.47
Risk	High	Medium

securiCAD®: Die Story

Zu den kritischen Infrastrukturen zählen beispielsweise die Sektoren Energie- und Wasserversorgung, Telekommunikation, Gesundheitswesen, Bank- und Versicherungswesen, sowie die Nahrungsmittelversorgung. Wie hoch der Schutzbedarf für IT-Netze gesehen wird, belegt unter anderem der globale Risikoreport 2016 des Weltwirtschaftsforums. Er stellt die weltweite Gefährdung durch Cyberangriffe auf Informationssysteme auf eine höhere Stufe als die omnipräsente Terrorgefahr!

Netzwerkmodellierung und Angriffssimulation mit securiCAD®

securiCAD® ist eine neuartige Software, mit deren Hilfe komplexe IT-Netzwerke modelliert werden können. Aber nicht nur Büronetzwerke, sondern insbesondere auch Netzwerke, die in kritischen Infrastrukturen vorkommen, wie zum Beispiel SCADA-Netze. Die Stärke von securiCAD® ist, dass securiCAD® Angriffe auf Netzwerke simulieren kann.

Die Software liefert eine Analyse über Schwachstellen im Netzwerk und eine Abschätzung, wie lange ein Angreifer benötigt, um das Netzwerk zu übernehmen. Änderungen im Netzwerk, zum Beispiel der Einbau einer neuen Firewall, können dann ebenso simuliert werden. So kann in einem Vorher-Nachher-Vergleich festgestellt werden, ob Sicherheitsmaßnahmen wirklich den Effekt erzielen, den sie erzielen sollen. Das verhindert Fehlinvestitionen in Maßnahmen, die keine wesentlichen Verbesserungen erzielen, und lässt Netzwerkbetreiber viel besser die Risiken einschätzen, die in einem Netzwerk stecken. Genau wie kein Ingenieur eine Brücke ohne penibelste Simulation der Statik baut, werden in Zukunft IT-Netze auch nicht ohne eine ingenieurmäßige Risiko- und Schwachstellenanalyse auskommen.

ICS implementiert und berät

Wir übernehmen für Sie die Modellierung Ihres Netzwerkes, führen die Simulationen durch und liefern Ihnen einen Ergebnisreport, der Ihrem Management vorgestellt werden kann. Und, natürlich geben wir Ihnen Empfehlungen, mit welchen Maßnahmen den gefundenen Schwachstellen entgegengewirkt werden kann. Dazu gehören, neben den technischen Netzwerkaspekten, auch organisatorische Maßnahmen, Dokumentationen und die Durchführung von Schulungen und Trainings. Gerne etablieren wir gemeinsam mit Ihnen einen Prozess zur regelmäßigen Wiederholung der Analysen inklusive aller in der Zwischenzeit angefallenen Änderungen in Ihrem Netz. So stellen Sie sicher, stets einen Überblick über die Gefährdungslage in Ihrem Netz zu haben, und weisen so ein geordnetes IT-Risikomanagement nach.

Neben der Beratung offeriert die ICS GmbH auch die Übernahme Ihrer Infrastruktur-Modellierung. Mittels eines Netzwerkscanners, eines Enterprise Asset Management Tools oder eines Netzwerksplans, erfassen wir Ihre Infrastruktur und überführen diese schnell und einfach in securiCAD®. Das spart Arbeit, Zeit und damit Kosten bei der Netzwerkmodellierung.

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

>>ICS-Downloads

Kontakt

ICS GmbH
Sonnenbergstr. 13
70184 Stuttgart

T +49 711 2 10 37 00
industry@ics-gmbh.de
www.ics-gmbh.de