

Das fehlende Glied **Ihrer** **Cyberabwehr**

Führen Sie in nur wenigen Stunden
eine realistische Übung zur Reaktion
auf Cybersicherheitsvorfälle durch –
**unter Beteiligung aller verantwortlichen
Personen.**



Sind Sie auf einen Cyberangriff vorbereitet?

Die Abhängigkeit der Gesellschaft vom Cyberraum nimmt stetig zu. Der Cyberraum gilt als fünfter militärischer Operationsraum, in dem die Einsatzbereitschaft der Streitkräfte durch geeignete Ausbildung und Übungen sichergestellt werden muss. Cyberkriminelle werden immer versierter und dreister, und ihre Angriffsmethoden und -vektoren werden zunehmend ausgefeilter.



Training zur Cyberabwehr ist auch für zivile Organisationen und Institutionen erforderlich. Neben erheblichen finanziellen Verlusten können Cyberangreifer Schäden verursachen, die kritische Infrastrukturen, Versorgungseinrichtungen, Dienstleistungen und sogar Menschenleben gefährden.

Organisationen investieren erhebliche finanzielle Mittel in technische und organisatorische Maßnahmen zur Prävention von Cyberangriffen.

Prävention ist wichtig. Fachleute betonen jedoch, dass sich die Sicherheitsstrategie eines Unternehmens nicht allein darauf beschränken sollte, sämtliche Cyberangreifer fernzuhalten. Was geschieht, wenn es trotz aller Maßnahmen zu einem Angriff kommt und Ihre Organisation mit einem Cybersicherheitsvorfall konfrontiert ist?

Können Sie dessen Ursache korrekt ermitteln? Zahlreiche Studien zeigen, dass zwischen dem Auftreten eines Vorfalls und seiner Erkennung im Durchschnitt Monate vergehen. Auf die Erkennung folgt die Analyse der Ursache des Vorfalls.

Wie gut sind Sie darin, Vorfälle einzudämmen,

ihre eigentlichen Ursachen zu beseitigen und Informationssysteme sowie den Geschäftsbetrieb wiederherzustellen?

Anders als bei Bränden, Erdbeben oder auch Pandemien gibt es bei Cyberangriffen ein konkretes Angriffsziel und einen aktiven Angreifer, der sein Vorgehen an Ihre Abwehrmaßnahmen anpassen kann.

Üben Sie Szenarien für Cybersicherheitsvorfälle und verbessern Sie Ihre Abwehrtaktiken, -techniken und -verfahren anhand der gewonnenen Erkenntnisse? Bei der Abwehr von Cyberangriffen spielt Technologie zweifellos eine wichtige Rolle. Der entscheidende Faktor bleibt jedoch der Mensch. Besondere Aufmerksamkeit verdienen diejenigen, die Vorfälle bewältigen und Entscheidungen auf operativer und strategischer Ebene treffen.

Training und Übungen

Wie bereits erläutert, lässt sich ein Vorfall nie vollständig ausschließen. Wen hätten Sie dann lieber am Steuer: ein Team, das bereits Erfahrung hat, oder eines, das zum ersten Mal mit einem Vorfall konfrontiert ist? Da vergleichsweise wenige Menschen bereits einen solchen Vorfall erlebt haben, können diejenigen ohne diese Erfahrung sie nur durch Übungen gewinnen.

Viele anspruchsvolle Tätigkeiten erfordern Training. Feuerwehrkräfte erreichen Schnelligkeit und Effizienz durch regelmäßige Notfallübungen. Chirurgen assistieren zunächst bei Operationen, arbeiten anschließend unter Aufsicht und operieren erst danach selbstständig. Fluglotsen trainieren an Simulatoren, in denen „Pseudopiloten“ den Flugverkehr simulieren. Die Ausbildung von Generälen ist noch komplexer und kostspieliger. Eine ähnliche Herausforderung stellt das Training von Teams zur Reaktion auf Cybersicherheitsvorfälle dar.

Die Reaktion auf einen Cybersicherheitsvorfall ist eine anspruchsvolle Aufgabe, bei der viele Menschen und Aktivitäten koordiniert werden müssen. Manche Aktivitäten dauern lange, und



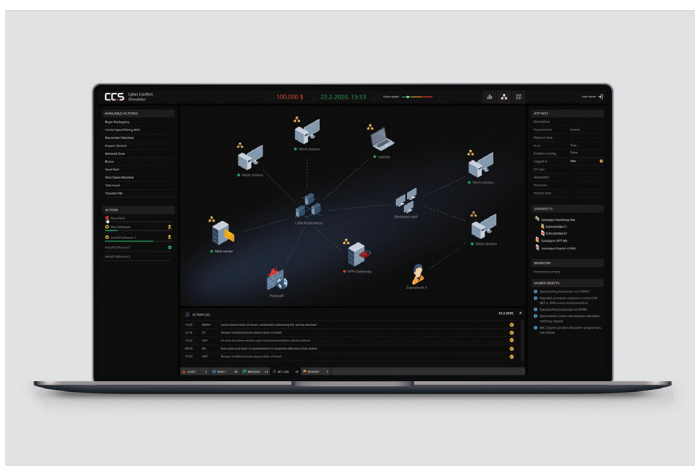
ihre Ergebnisse sind für Entscheidungen über die nächsten Schritte maßgeblich. Vorfälle können Tage, Wochen oder noch länger andauern. Die erforderlichen Entscheidungen gehen in der Regel über die IT hinaus und betreffen den Geschäftsbetrieb. Dabei werden Personen in zentralen geschäftlichen Funktionen einbezogen.

All dies macht die Organisation und Durchführung von Übungen anspruchsvoll. Es ist schwierig, Schlüsselpersonen für längere Übungen

von ihren regulären Aufgaben freizustellen. Daher lassen sich solche Übungen kaum häufig genug durchführen, um innerhalb eines angemessenen Zeitraums Erfahrung aufzubauen.

Auch Regulierungsbehörden haben die Bedeutung von Übungen erkannt. Für Organisationen von besonderer Bedeutung, etwa Betreiber kritischer Infrastrukturen, sind Übungen heute häufig vorgeschrieben. Die EU-Richtlinien NIS und NIS2 nennen Übungen als eine Möglichkeit, sich wirksam auf einen möglichen Vorfall vorzubereiten.

All diese Herausforderungen führten zur Entwicklung von Cyber Conflict Simulator - einem interaktiven Simulator, der einen anderen Ansatz für die Reaktion auf Cybersicherheitsvorfälle verfolgt.



Cyber Conflict Simulator (CCS) ist ein Softwaresystem für Personen, die im zivilen oder militärischen Bereich für die Bewältigung von Cybersicherheitsvorfällen verantwortlich sind.

SO FUNKTIONIERT CCS

Cyber Landscape

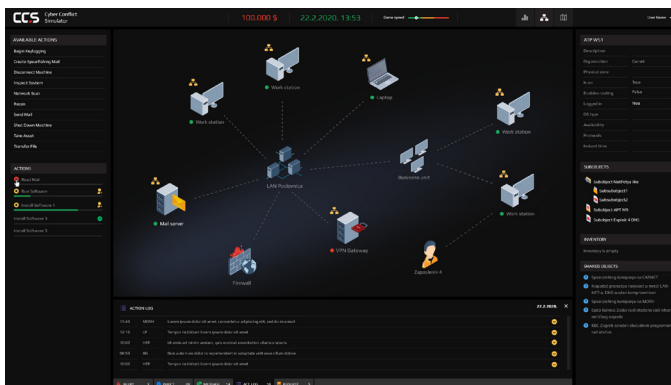
Stellen Sie sich vor, Sie könnten Ihre IT- und Geschäftssysteme in eine virtuelle Umgebung übertragen. Dort lassen sie sich so konfigurieren, dass sie genauso funktionieren wie in der realen Welt. Mit CCS können Sie beschreiben, wie geschäftliche Dienstleistungen oder Produktionsprozesse von den angegriffenen IT-Systemen abhängen und welche Folgen deren Störung hat.

Das IT-System wird durch Objekte wie Computer, Server, mobile Geräte, Netzwerke, Betriebssysteme, Software, Dienste, Dateien, Datenbanken und SCADA-Systeme abgebildet. CCS ermöglicht außerdem die Definition von Abhängigkeiten von externen Diensten. Diese Dienste können durch einen Cybersicherheitsvorfall gestört werden oder einem Angreifer als Einstiegspunkt dienen.

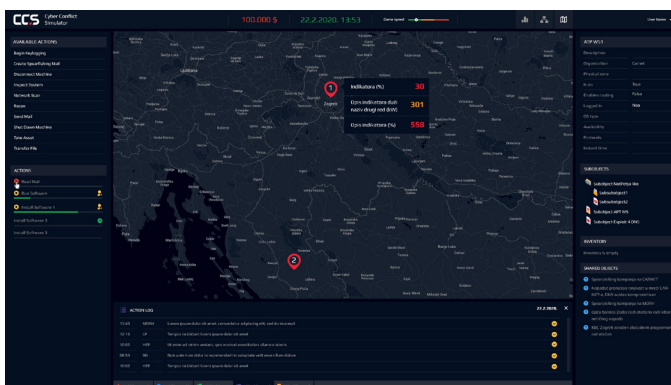
Menschen sind ein wichtiger Bestandteil jeder Organisation - Systemadministratoren, Spezialisten für digitale Forensik, Techniker, Analysten und alle weiteren Mitarbeitenden. Sie bilden ein virtuelles Team, das die Teilnehmenden während der Simulation führen. Angreifer lassen sich so modellieren, dass sie unterschiedliche Bedrohungsquellen darstellen, darunter Staaten, kriminelle Gruppen und Einzelpersonen.

Simulation

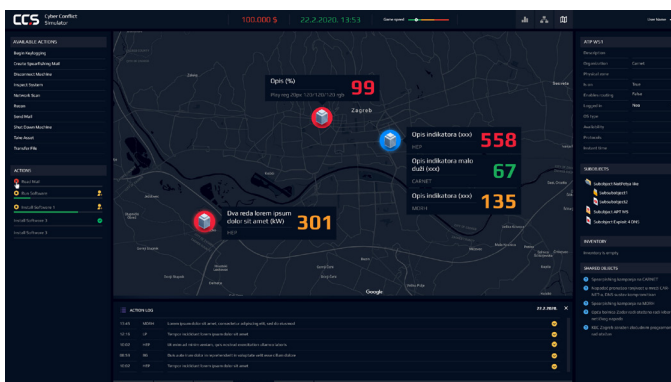
Eine realistische Übung muss die Ereignisse in der IT-Infrastruktur, in der das Problem entsteht, präzise modellieren. Auch die geschäftlichen Auswirkungen müssen abgebildet werden, da sie die tatsächlichen Schäden oder Verluste widerspiegeln, die auftreten können.



Die Simulation kann vordefinierten Szenarien und geplanten Schritten folgen oder unter aktiver Beteiligung eines Red Teams stattfinden. Die Übung kann mit dem Beginn der Angriffsaktivitäten einsetzen oder erst später, wenn der Vorfall erkannt wird und der Angreifer bereits einige seiner Ziele erreicht hat. Den Startpunkt legt die Person fest, die das Übungsszenario erstellt.



An der Simulation können mehrere Teilnehmergruppen mitwirken. Auch mehrere Organisationen können an der Übung teilnehmen. Jede von ihnen sieht dabei nur die Informationen, die ihr in einer realen Situation zur Verfügung stünden.



Die Teilnehmenden weisen den Mitgliedern ihres virtuellen Teams Aufgaben zu. Diese Teammitglieder bezeichnen wir als Akteure. Die Fähigkeiten eines Akteurs bestimmen, welche Aufgaben er ausführen kann und wie lange diese dauern — genau wie im realen Leben.

Die Akteure berichten über ihre Arbeit und deren Ergebnisse. Auf dieser Grundlage entscheiden die Teilnehmenden über die nächsten Schritte zur Bewältigung des Vorfalls.

Während der Übung müssen die Teilnehmenden häufig auf die Ergebnisse der Aktivitäten ihrer Akteure warten. In diesen Phasen kann die Simulation beschleunigt und jederzeit wieder verlangsamt werden. Dadurch lässt sich die Übung in deutlich kürzerer Zeit durchführen, als die entsprechenden Ereignisse in der Realität dauern würden. Mit CCS kann ein Cyberangriff, der Tage oder Wochen dauern würde, in nur wenigen Stunden simuliert werden.

Sobald der virtuelle Cyberraum definiert ist, können Sie beliebig viele Übungen mit unterschiedlichen Szenarien durchführen. Die Übung wird wesentlich durch die verfügbaren Ressourcen des Angreifers und die von ihm eingesetzten Angriffstechniken bestimmt. Daraus ergibt sich eine große Vielfalt möglicher Übungsszenarien.



Alle Schritte und Ereignisse der Übung werden protokolliert und im Simulationsbericht dokumentiert. Dies ermöglicht Verbesserungen an der Abwehrstrategie, den Taktiken, Techniken, Verfahren und dem gesamten System.

Für die Cyberabwehr sind zahlreiche Fragen entscheidend. Lässt sich ein Angriff frühzeitig erkennen? Wie leicht kann sich ein Angreifer innerhalb Ihrer Organisation bewegen, um sein Ziel zu erreichen? Die Liste ließe sich fortsetzen.

Antworten finden Sie am besten, indem Sie Ihre Abwehr auf die Probe stellen. CCS ist ein wertvolles Werkzeug zum Testen Ihres IT-Systems. Sie können verschiedene Angriffe auf Ihre Organisation simulieren und prüfen, wie leicht Sie einen Angriff erkennen und eindämmen können und ob sich letztlich nachvollziehen lässt, was tatsächlich geschehen ist.

Sie können Zero-Day-Schwachstellen in beliebige Komponenten Ihres Systems einführen und testen, wie diese sich im Angriffsfall auf Ihre Abwehr auswirken.

Die wichtigsten Funktionen



FLEXIBILITÄT

Erstellen Sie einen virtuellen Cyberraum, der Ihrem realen Informationssystem vollständig entspricht.



INTERAKTIVITÄT

Das Ergebnis der Simulation hängt vollständig von den Handlungen der Teilnehmenden ab.



ZEITSTEUERUNG

Beschleunigen Sie die Simulation jederzeit, um die Übung zu verkürzen und Zeit zu sparen.



SKALIERBARKEIT

Modellieren Sie komplexe Systeme unter Einbeziehung aller verbundenen Organisationen.



ERWEITERBARKEIT

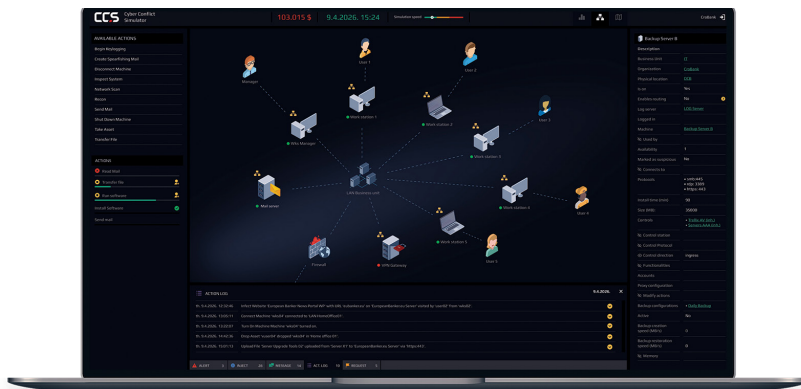
Erweitern Sie das System mithilfe eines Plug-in-Mechanismus um neue Objekte, Aktionen und Kontrollmaßnahmen.



GEWONNENE ERKENNTNISSE

Analysieren Sie in der Nachbereitung die während der Übung durchgeführten Schritte und verbessern Sie so die Abwehrtaktiken und -techniken Ihres Teams.

Mit Training zur Einsatzbereitschaft



CCS

**Das fehlende
Glied Ihrer
Cyberabwehr**

Mit Utilis CCS können Sie bewerten, wie gut Ihre Organisation auf Cybersicherheitsvorfälle vorbereitet ist. Sie testen die Robustheit Ihres IT-Systems und bereiten den wichtigsten Bestandteil Ihrer Abwehr vor – Ihre Mitarbeitenden.

CCS richtet sich an Personen, die im zivilen oder militärischen Bereich für die Bewältigung von Cybersicherheitsvorfällen verantwortlich sind. Es simuliert unterschiedliche Arten von Cyberangriffen auf Ihr Informationssystem und ermöglicht die Definition eines virtuellen Cyberraums aus verschiedenen Objekten.

Mit CCS können Sie ganz einfach

- Die Reaktion und Leistungsfähigkeit Ihres Systems und Ihres Teams zur Reaktion auf Cybersicherheitsvorfälle im Angriffsfall bewerten
- Ihre Verfahren zur Reaktion auf Cybersicherheitsvorfälle und Ihre Kommunikationspläne testen
- Zeit und andere Ressourcen bei der Übungsvorbereitung sparen und dadurch mehr Übungen mit weniger Aufwand durchführen
- Cybersicherheitsvorfälle, die Tage oder Wochen dauern würden, in wenigen Stunden simulieren

- Durch Übungen mit unterschiedlichen Angriffsszenarien Erfahrung und Fähigkeiten erwerben
- Das Bewusstsein für Bedrohungen Ihres IT-Systems stärken

„Aus Fehlern lernt man“, heißt es. Fehler bei realen Cybersicherheitsvorfällen können sehr teuer werden. Deshalb ist es besser, sie zuerst in Übungen zu machen. Wir haben CCS so entwickelt, dass es sehr einfach zu bedienen ist. Über ein Plug-in-System lässt es sich zudem leicht erweitern.

Bereits in der Anfangsphase wurde CCS von der Europäischen Verteidigungsagentur (EDA) als innovatives Dual-Use-Projekt mit militärischen und zivilen Anwendungsmöglichkeiten anerkannt und für technische Unterstützung ausgewählt.

Vereinbaren Sie eine Übung

Ein Expertenteam von Utilis und FER kann alles vorbereiten, was zur Durchführung einer Übung erforderlich ist - bei minimalem Aufwand für Ihre Organisation.

Kontaktieren Sie uns bei weiteren Fragen, fordern Sie eine Präsentation an oder vereinbaren Sie eine auf Ihre Organisation zugeschnittene Übung.

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd.

Fallerovo šetalište 22

10000 Zagreb, Kroatien

www.utilis.biz

ccs.utilis.biz



**Kofinanziert von der
Europäischen Union**