Cyber Defence : ein neuer Ansatz

Autor(en): **Müller, Peter**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **182 (2016)**

Heft 3

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-587021

Cyber Defence: Ein neuer Ansatz

Zivile und militärische Computer-Netzwerke sind ständigen Angriffen ausgesetzt. Die Methodenvielfalt stellt eine grosse Herausforderung dar. Frühzeitiges Erkennen von Anomalien im Datenverkehr liefert einen möglichen Sicherheitsansatz. Florian Schütz, Business Developer Cyber & Intelligence, stellt das neue Instrument von RUAG Defence in einen grösseren Zusammenhang.

Peter Müller, Redaktor ASMZ

Peter Müller: RUAG Defence hat kürzlich in Bern erste Ausbildungen in Ihrer neuen «Cyber Training Range» durchgeführt. Welche Auslöser stehen hinter diesem Angebot und welches Zielpublikum wird angesprochen?

Florian Schütz: Mit unserer Ausbildung richten wir uns an Spezialisten, technische Operatoren, aber auch an Führungskräfte und Supportorganisationen. Unser Training hat zum Ziel, das operationelle Verhalten zu verbessern, um sowohl das Verständnis als auch die spezifischen Fähigkeiten in Zusammenhang mit zukünftigen Sicherheitsanforderungen zu optimieren.

Durch die zunehmende Verschmelzung von Technologie mit dem Alltag ist die Trennlinie zwischen Cyber- und anderen Sicherheitsthemen unschärfer geworden. In unserer Tätigkeit haben wir festgestellt, dass generell das Verständnis, gerade auch der nicht technischen Faktoren, ungenügend und nicht weitreichend genug ist. Genau dieses Verständnis aber ist es, was einen effizienten und effektiven Sicherheitszuwachs erst ermöglicht. Dieses ungenutzte Potential wollen wir unseren Kunden vermitteln.

RUAG Traffic Analyzer

Der RUAG Traffic Analyzer ist eine hochmoderne Lösung zur Erkennung einer kundenseitigen Infizierung durch Analyse der vorgelagert generierten Daten. Er ermöglicht eine benutzerorientierte Sichtbarkeit, ungeachtet der Endgeräteplattform. Dank nahtloser Integration – da bestehende Protokolle genutzt werden, ist keine Installation von Sensoren notwendig – werden folgende Ereignisse mit hoher Zuverlässigkeit entdeckt:

- Infektiöse Malware: Spambots, Zombie Hosts, Viren-/Würmer-Propagierung und verdeckte Kanäle;
- Ab- und eingehender (Distributed) Denial of Service;
- Session-Hijacking, Phishing-Attacken und andere Hacking-Techniken;
- Drive-by-, E-Mail- und CSS-Vektoren;
- Ungewöhnliche Nutzung von Applikationen;
- Ungewöhnliche Aufforderung zur Ressourcenfreigabe.

Quelle: RUAG Defence

Klickt man im Internet auf «Cyber Security Training», so ergeben sich rund 36 Mio. Treffer. Das sieht nicht nach einem Nischenprodukt aus. Folgt die RUAG somit einem grossen Markttrend oder bieten Sie spezifische Einzigartigkeiten an?

Die meisten Konkurrenten bieten rein technische Ausbildungen oder reine Führungstrainings an. Des Weiteren beziehen sich die Angebote in der Regel sehr stark auf theoretische Grundlagen. Das Erlernte kann demnach nicht vertieft werden.

Andere Konkurrenten bieten Hackerspiele an, bei denen Teams von echten Angreifern attackiert werden. Dieses Angebot generiert aber einen eher geringen Mehrwert, da die Szenarien nicht reproduzierbar sind und die Performance stark von den einzelnen Kursteilnehmern abhängt. Wir haben eine Trainingsmethodik entwickelt, welche die positiven Elemente der beiden genannten Ausbildungen gesamtheitlich miteinander verknüpft und repetierbar ist. Darüber hinaus haben wir die Möglichkeit, Führungskräfte, technische Operatoren und Spezialisten im Verbund zu trainieren.

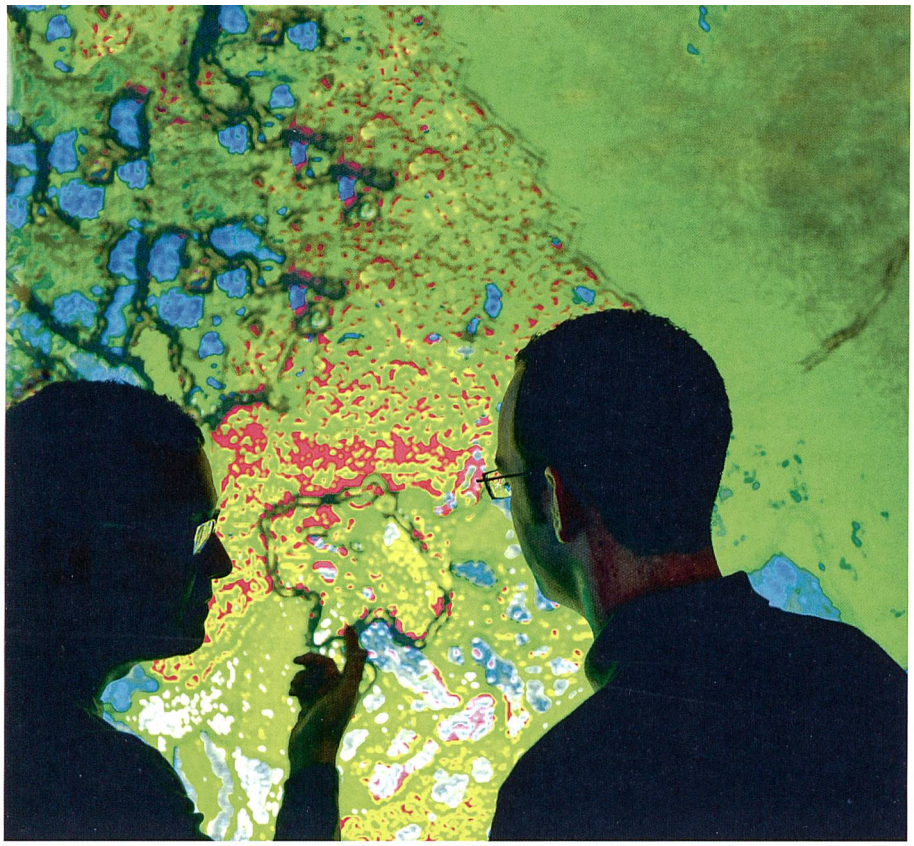
Im Zentrum Ihres neuen Angebots steht der sogenannte «RUAG Traffic Analyzer (RTA)». Können Sie uns dessen Funktionsweise sowie die Darstellung der Ergebnisse kurz erläutern? Gibt es leicht erkennbare, typische Formen von Netzwerkanomalien?

Der RUAG Traffic Analyzer verwendet Methoden wie beispielsweise statistische Analysen, um Anomalien im Datenverkehr zu erkennen. Dies im Gegensatz zu den meisten Erkennungsmethoden, die bereits bekannte Muster zur Detektion von Angriffen verwenden. Der RUAG Traffic Analyzer ist somit in der Lage, schnell mutierende und noch unbekannte Angriffe zu erkennen. Dabei ist es wichtig zu verstehen, dass eine Anomalie immer durch den Kontext definiert wird. Ein Beispiel: In einer Client-Server-Architektur, also wenn Sie Mediendaten über Internet-TV von einem Anbieter beziehen, fliessen viele Daten vom Anbieter zu Ihnen. Bei Peer-to-Peer-Netzwerken, wie sie oft für das meist illegale Tauschen von Musik und Filmen verwendet werden, ist hingegen jeder Teilnehmer Anbieter und Konsument gleichzeitig. Der Verkehr fliesst also in etwa gleichmässig in beide Richtungen. Eine allfällige Anomalie ergibt sich demnach aus der Art Ihrer Organisation. Wenn Sie als Unternehmen keine Peer-to-Peer-Programme zulassen, wäre das Vorkommen eines solchen Verkehrs konsequenterweise eine Anomalie. Leider ist dies in der Praxis meistens deutlich komplexer und nicht immer eindeutig zu bestimmen. Unsere Stärke liegt im Anpassen der Technologie an die individuellen Kundenbedürfnisse und im Erkennen global gültiger Anomaliemuster.

Zusammenarbeit?

Eine effiziente Cyber Defence bedingt die enge Zusammenarbeit zwischen Staat und Wirtschaft. Es mutet deshalb etwas eigenartig an, dass die zuständige Stelle im VBS über das neue Produkt der RUAG weder orientiert noch involviert ist.

Gemäss Ihrem Anspruch wollen Sie «zukünftige Bedrohungen mit hoher Wahrscheinlichkeit erkennen». Dem stehen die Innovationsgeschwindigkeit sowie die Methodenvielfalt das heisst die stets neuen und unbekannten Arten von Cyber-An-



Cyber Security: Erkennen von Anomalien im Datenverkehr. Bild RUAG Defence

griffen gegenüber. Wie begegnet die RUAG diesem Dilemma?

Der Fehler, der oft gemacht wird, ist, dass man sich zu sehr auf die Angriffe fokussiert. Es ist korrekt, dass diese immer anders aussehen und der Innovationskraft von Gegnern kaum Grenzen gesetzt sind. Verschiebt man jedoch diesen Fokus auf den Angreifer und dessen Motivation, dann ergeben sich auf einmal Konstanten. Kombiniert man dies mit abstrakten Mustern aus bekannten Angriffen und gibt noch etwas Mathematik, in Form von Statistik oder Machine-Learning hinzu, kann man wesentlich mehr erkennen. Wir kennen dies bereits von konventionellen, physikalischen Angriffen. Ein Beispiel: Eine Nation wird mit einem Flugkörper beschossen. Der Angriff ist also klar erkennbar. Es spielt aber eine sekundäre Rolle, mit welcher Waffe der Angriff erfolgt, zumal die Attacke sowieso Schaden anrichten wird.

Die Auffassung scheint weit verbreitet, dass die Umsetzung einer umfassenden Cyber-Sicherheitsstrategie, eine sichere IT-Architektur sowie eine gewissenhafte Schulung des Personals jeden Cyber-Angriff ins Leere laufen lassen. Täuscht dieses Sicherheitsempfinden?

Definitiv. Man muss sich von der Idee perfekter Sicherheit verabschieden. Absolut ist im Cyberspace gar nichts. Es gibt keinen totalen Schutz; es gibt nur adäquaten Schutz. Aber alles, was getan wird, erhöht die Überlebensfähigkeit im Cyberspace. Das Spektrum reicht vom Verhindern, dass man sich in Gefahr begibt oder entdeckt wird, bis zum schnellen Wiederherstellen nach einem vernichtenden Angriff. Dies entspricht klassischen militärischen Operationen.

Mit der Erkennung von sicherheitsrelevanten Benutzeraktivitäten und der Identifikation von infizierten Endgeräten taucht irgendwie das Bild von «big brother» und «gläsernen Mitarbeitenden» auf. Entstehen daraus keine Konflikte zum Daten- und Persönlichkeitsschutz?

Konflikte entstehen, wenn man den Einsatzraum nicht differenziert betrachtet. Je nach Einsatzraum, Ort, Art und Gefährdungslage gelten unterschiedliche gesetzliche Bestimmungen. Diese sind bei der Planung mit zu beachten. Des Weiteren gibt es ethische und moralische Faktoren, die abhängig vom Einsatzort und -zweck zu beachten sind. Wir Schweizer legen beispielsweise grossen Wert auf die Privatsphäre und sie ist ein wichtiger Pfeiler unserer Gesellschaft. Die Briten sind da liberaler. Es ist also wichtig, sensibel zu sein und darauf zu achten, dass die Mitarbeitenden nicht gegen das System arbeiten und so die Sicherheit negativ beeinflussen. Wir bei der RUAG sind uns dieses Balanceaktes bewusst. So schützen wir bei der Datenverkehrsanalyse mit dem Traffic Analyzer die Privatsphäre maximal, indem wir zur Identifikation von Anomalien vor allem auf technische Parameter setzen.

Die Diskussionen um eine nationale Cyber-Defence-Strategie machten deutlich: Die einen befürworten die Übernahme von (Mit-)Verantwortung der öffentlichen Behörden; die andern appellieren an die Eigenverantwortung der Unternehmen sowie der Nutzer. Welches Vorgehen befürwortet die RUAG?

Der Bund verfolgt mit der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) drei Hauptziele. Dazu gehören die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich, die Erhöhung der Widerstandsfähigkeit kritischer Infrastrukturen sowie die wirksame Reduktion der Risiken. Um diese Aufgabe in einer hoch vernetzten Gesellschaft zu bewältigen, braucht es eine klare Aufgabenteilung und eine enge Zusammenarbeit zwischen Staat und Wirtschaft. Der Staat kann vor allem in den Bereichen Risikobeurteilung und Lageeinschätzungen die Wirtschaft, die Betreiber kritischer Infrastrukturen und die Behörden unterstützen. Dazu wird ein intensiver und systematischer Informationsaustausch vorausgesetzt. Die systemrelevanten Unternehmen unterliegen bereits heute spezifischen Regeln und haben einen auferlegten Handlungsbedarf. Viele der grösseren Unternehmen sind sich der Problemstellung bewusst und handeln heute in eigener Verantwortung. In der Schweiz gibt es aber sehr viele kleinere und mittlere Unternehmen mit beschränkten finanziellen Mitteln. Diese sind auf sichere kommerzielle Sicherheitsinfrastrukturen und die Unterstützung durch die branchenspezifischen Verbände angewiesen.

Zum Abschluss noch ein kurzer Blick in die Zukunft: RUAG entwickelt zurzeit ein Cyber Security Management Informationssystem. Was wird dieses Instrument beinhalten und wann sollte es voraussichtlich verfügbar sein?

Die RUAG wird mittelfristig ein Cyber Security Management Informationssystem auf den Markt bringen, das speziell auf die Bedürfnisse des Top-Managements zugeschnitten ist. Ziel des Systems ist, dass sich nicht nur Cyber-Experten, sondern eben auch das Management, innert kürzester Zeit einen Überblick verschaffen können und dadurch erkennen, in welchem Stadium sich die interne Cyber Security befindet. Dies ist ein weiterer Schritt, um die cyberspezifische Sicherheit innerhalb der Organisationen sukzessive zu optimieren. ■