Führungsunterstützungsbasis : Schutz und Überwachung der IKT-Systeme

Autor(en): **Ruef, Marc / Schmidlin, Diego**

Objekttyp: **Article**

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

Band (Jahr): **186 (2020)**

Heft 11

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-905668

Führungsunterstützungsbasis: Schutz und Überwachung der IKT-Systeme

Alle unsere Aktivitäten fokussieren darauf, unseren Schutz stetig auszubauen, Schwachstellen zu erkennen sowie Cyber-Angriffe zu detektieren und abzuwehren. Der Bereich Cyber Security trägt unter der Leitung des CISO (Chief Information Security Officer) die Gesamtverantwortung für die IKT-/Informationssicherheit und den Schutz der eigenen IKT-Infrastruktur vor Cyber-Angriffen.

Diego Schmidlin, Chef Cyber Security, CISO FUB, beantwortet die Fragen von Marc Ruef, Kolumnist ASMZ.

Ruef: Wo sehen Sie Ihre Kernaufgabe als CISO und Chef Cyber Security der FUB?

Schmidlin: Wir überwachen permanent die eigenen IKT-Systeme und intervenieren bei Vorfällen sofort. Weiter erstellen wir für die Prävention die Vorgaben und sorgen dafür, dass diese umgesetzt und eingehalten werden. Die Sensibilisierung der Mitarbeitenden und der Miliz zum Thema Cyber-Sicherheit und Informationssicherheit fallen ebenfalls in unser Aufgabengebiet.

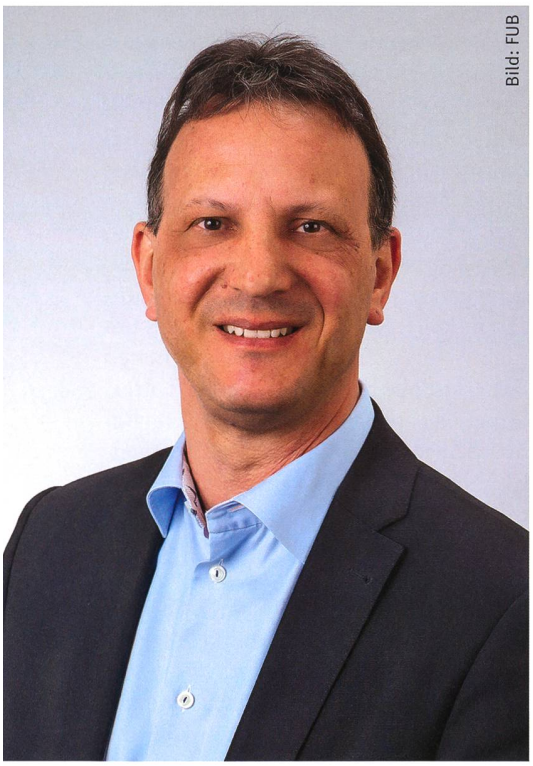

Bild: FUB

Diego Schmidlin, Chief Information Security Officer Führungsunterstützungsbasis.

Was ist der Unterschied zum gleichen Posten bei einem Unternehmen in der Privatwirtschaft?

Die militärische Systemlandschaft besteht einerseits aus festen Installationen, andererseits kommen teilmobile und mobile Netzte sowie IKT-Systeme dazu. Dies bedeutet, dass sich je nach Operation und Einsatz der Armee die Systemlandschaft dauernd verändert. Weiter haben die einsatzrelevanten Systeme wie Führungsinformationssysteme oder Waffensysteme einen viel höheren Schutzbedarf als vergleichbare zivile Mittel. Ältere Systeme bringen vielfach nicht das gewünschte Schutzniveau mit, diese müssen dann zusätzlich gehärtet und überwacht werden.

Wie gehen Sie mit Vulnerability Management, dem Bearbeiten von neuen und gefundenen Schwachstellen in Systemen, um?

Wir suchen systematisch nach bekannten und unbekannten Schwachstellen bei den eingesetzten Systemen oder in unseren Konfigurationen. Entdeckte Schwachstellen werden erfasst, untersucht, dokumentiert, wenn möglich behoben oder isoliert. Dies ist eine fortlaufende Tätigkeit, welche viel Zeit und Expertise erfordert. Bei verschiedenen Gelegenheiten spannen wir auch mit externen Partnern und anderen Sicherheitsorganisationen in der Bundesverwaltung zusammen und tauschen Informationen mit ihnen aus.

Was würde die Beschaffung neuer Kampfflugzeuge für Ihren Auftrag bedeuten?

Mit den neuen Kampfflugzeugen werden auch die benötigten IKT-Systeme für die Wartung und Vorbereitung von Missionen mitgeliefert. Dort, wo es Schnittstellen gibt, werden die neuen Systeme in die bestehende Systemlandschaft integriert und gegenseitig abgesichert.

Die FUB steht gegenwärtig in der Kritik, die minimalen Sicherheitsanforderungen für gewisse Systeme nicht gewährleisten zu können. Wo liegt das Problem, dass beispielsweise gewisse Zugänge nicht dokumentiert sind und teilweise veraltete Mechanismen (z.B. SMBv1) eingesetzt werden?

Ein Ausbau des IKT-Schutzes bei veralteten Systemen wäre ökonomisch nicht sinnvoll. Die FUB ist im Moment dabei, alle Ressourcen auf den Aufbau einer neuen IKT-Umgebung zu konzentrieren. In der bestehenden Systemlandschaft halten wir das aktuelle Schutzniveau ein und passen dieses – wo nötig – an die aktuellen Bedrohungen an. Eine ausführliche Antwort würde den Rahmen hier sprengen. Wir haben dazu ein Positionspapier verfasst, es ist unter armee.ch/ikt-sicherheit zu finden.

«Durch uns betreute einsatzrelevante Systeme wie Führungsinformationssysteme oder Waffensysteme haben einen viel höheren Schutzbedarf als vergleichbare Mittel im zivilen Bereich.»

Verwaltung und bundesnahe Organisationen tun sich selten mit einem hohen Mass an Flexibilität und Agilität hervor. Inwiefern macht das Ihren Auftrag schwieriger?

Die schnelle Entwicklung im Bereich Cyber Security stellt eine Herausforderung für alle IKT-Betreiber dar. Das for-

dert auch meine Mitarbeitenden stark. Wir müssen häufig kreativ sein, weil die gewünschte Lösung nicht einfach am nächsten Tag auf dem Tisch liegt. Ist eine Beschaffung einmal sehr dringend, erhalten wir vom Armeestab und der Beschaffungsstelle armasuisse die nötige Unterstützung.

Wie nehmen Sie den noch relativ jungen Cyber-Lehrgang der Armee wahr? Halten Sie in der Truppe ebenfalls Ausschau nach Talenten, die Ihre Organisation ausserhalb der WKs unterstützen können?

Der Cyber-Lehrgang wurde innert kürzester Zeit zusammen mit Partnern aus Industrie und Bildung gegründet. Nach Abschluss des Lehrgangs kann die Berufsprüfung zum «Cyber Security Specialist» mit eidgenössischem Fachausweis abgelegt werden. Die Absolventen erhalten zudem 21 ETCS gutgeschrieben, die sie im Bachelor für Information & Cyber Security an der Hochschule Luzern einsetzen können. Die in der Weiterausbildung zum Wachtmeister absolvierte Führungsausbildung kann ebenfalls mit einer zivil anerkannten Bescheinigung abgeschlossen werden. Etwas mehr als die Hälfte der Teilnehmenden des Cyber-Lehrgangs absolvieren ihren praktischen Dienst in der Abteilung Cyber Security. Die angehenden Wachtmeister bringen spannende neue Perspektiven ein und sind eine grosse Bereicherung für unsere Teams. Wenn sich nach dem Lehrgang ein Absolvent auf eine Stelle oder ein weiterführendes Praktikum bei uns bewirbt, dann freut uns das sehr. Ebenso wichtig ist, dass Schweizer Unternehmen gut ausgebildete Absolventen erhalten. Alle Involvierten können von dieser Win-Win-Situation profitieren.

Sie waren über 13 Jahre im IT- und Cyber-Security-Bereich der RUAG tätig. Das Jahr 2016 wird Ihnen sicher in schmerzlicher Erinnerung bleiben: Wie haben Sie den erfolgreichen Hack auf die Organisation erlebt?

Das war eine sehr anspruchsvolle Zeit und die Bewältigung eines so grossen Ereignisses eine riesige Herausforderung. Aus heutiger Perspektive konnten aber alle Beteiligten sehr viel über das Vorgehen und das Verhalten eines realen und sehr versierten Angreifers lernen. Dazu gehört die koordinierte Zusammenarbeit mit den Partnern und den Behörden sowie die Kommunikation zu den Mitarbeitenden, Bundesstellen, Kunden, Lieferanten und der Öffentlichkeit. Ich konnte vieles mitnehmen und kann die gewonnenen Erkenntnisse nun in der FUB gezielt einbringen.

Welches sind die Lehren, die aus diesem Zwischenfall, auch für Sie persönlich in Ihrer heutigen Position, gezogen werden können?

Der Schutz und die Überwachung der eigenen IKT-Systeme ist laufend an die neuen Bedrohungen aus dem Cyber-Raum anzupassen. Ein starkes Partnernetzwerk muss vor einem Cyber-Angriff bereits aufgebaut sein. Der Einsatz einer Taskforce oder des Krisenmanagements benötigt regelmässiges Training. Dabei können die verschiedenen Taktiken zur Beobachtung, Eindämmung und Abwehr eines Angriffs sowie die Zusammenarbeit mit den Partnern und die Führung der Kommunikation einstudiert werden.

«Im Ernstfall (Aktivdienst) sind für eine Armee heutzutage ihre offensiven Fähigkeiten für die Aufklärung und Wirkung in fremden IKT-Systemen nicht mehr wegzudenken.»

Sind Sie ein Befürworter von offensiven Aktivitäten und «Hack-Back»? Wären diese im RUAG-Fall gerechtfertigt gewesen?

Im Ernstfall (Aktivdienst) sind für eine Armee offensive Fähigkeiten für die Aufklärung und Wirkung in fremden IKT-Systemen heutzutage nicht mehr wegzudenken. Die militärischen Operationen können im Vorfeld und bei der Durchführung durch aktive Cyber-Fähigkeiten zusätzlich unterstützt werden. Der Einsatz von offensiven Cyber-Mitteln im Alltag ist in der Schweiz gesetzlich klar geregelt. Im Rahmen dieser Rechtsgrundlagen profitieren wir von unseren offensiven Fähigkeiten vor allem darin, dass wir so lernen, wie Cyber-Angriffe funktionieren. Dadurch können wir uns besser schützen und laufend verbessern.

Sollten neu gefundene Schwachstellen (0-days) geheim gehalten und exklusiv durch das VBS ausgenutzt werden – oder gilt es, diese öffentlich und damit der gesamten Security Community zugänglich zu machen?

Die Cyber Community profitiert vom regen Austausch von Informationen sehr. Entdeckte Schwachstellen (0-days) sollten aus meiner Sicht immer zumindest den Herstellern bekannt gegeben werden. Dazu bestehen heute bereits einige Bug-Bounty-Programme. Schwachstellen, welche durch uns gefunden werden, werden unseren Partnern kommuniziert und auch an die Hersteller weitergegeben. Umgekehrt profitieren wir auch vom Wissen unserer Partner.

Welches sind Themen, die Ihnen in Ihrer heutigen Rolle die grössten Herausforderungen bereiten?

Die Mitarbeitenden und die Miliz adäquat zu schulen und zu sensibilisieren ist ein ständiger Prozess. Schlussendlich können all unsere Systeme noch so gut geschützt sein, der Mensch spielt eine wesentliche Rolle bei der Verhinderung eines Angriffs über Spam-Mails, Social Media und infizierte Webseiten. Die heterogenen, historisch gewachsenen IKT-Infrastrukturen sind für alle grossen Organisationen eine Herausforderung. Einige Technologien, die heute bei der Armee noch im Einsatz sind, lassen sich auf Jahrzehnte zurückdatieren, während der technologische Fortschritt rasant zunimmt. Diese Rahmenbedingungen stellen die IKT-Sicherheit vor grosse Herausforderungen.

Was muss die Schweiz tun, um im Bereich Cyber vorne dabei sein zu können?

Generell braucht es genügend und sehr gut ausgebildete Fachexperten. Weiter ist die aktive Beteiligung an nationalen und internationalen Veranstaltungen wichtig, um neues Wissen aufzubauen und sich auch mit anderen Nationen messen zu können. Wir in der Armee sind hier bereits gut aufgestellt, wir arbeiten intensiv mit den Hochschulen zusammen und nehmen aktiv an nationalen und internationalen Übungen teil.

Vielen Dank, dass Sie sich für dieses Gespräch Zeit genommen haben. ■

Marc Ruef
Head of Research
scip AG, Zürich
5436 Würenlos