Cyber-Spezialisten der auf der US Air Base Ramstein residierenden U.S. Air Forces in Europe – Air Forces Africa werden im Warrior Preparation Center in der Air Station Einsiedlerhof bei Kaiserslautern in der Abwehr von Cyber-Angriffen geschult.

LUFTPOST

Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 096/18 – 06.0718

Cyber-Spezialisten der Air Force üben den Schutz des Informationsraumes

Von Airman 1st Class D. Blake Browning, 86th Airlift Wing Public Affairs
Kaiserslautern American, 24.05.18
(https://www.kaiserslauternamerican.com/cyber-airmen-unite-to-protect-information-space/)

Die im **Warrior Preparation Center in der Einsiedlerhof Air Station** (einem Schulungszentrum der Air Force auf dem Einsiedlerhof, einem Stadtteil im Westen Kaiserslauterns, s. https://en.wikipedia.org/wiki/USAFE_Warrior_Preparation_Center und http://www.wikiwand.com/en/USAFE_Warrior_Preparation_Center) durchgeführte **erste Schulung von Cyber-Spezialisten der (auf der Air Base Ramstein residierenden) U.S. Air Forces in Europe – Air Forces Africa / USAFE-AFAFRICA** (s. dazu auch https://en.wikipedia.org/wiki/United_States_Air_Forces_in_Europe_-_Air_Forces_Africa) endete am 11. Mai 2018.

"Zweck der Übung war es, die Fähigkeit unserer Cyber-Spezialisten zur Verteidigung unseres Cyber-Informationssystems durch Abwehr gegnerischer Angriffe zu trainieren," erläuterte Master Sgt. (Feldwebel) Daidric Young, der als Cyber Integration Manager der USAFE tätig ist.

Soldaten der **86th Communication Squadron (von der Air Base Ramstein,** s. http://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/433078/86-communications-squadron-usafe/ **)**, der **52nd Communications Squadron (von der Air Base Spangdahlem,** s. http://www.spangdahlem.af.mil/News/Features/Display/Article/730708/52nd-communications-squadron-keeps-spangdahlem-connected/ **)**, der **31st Communications Squadron (von der Air Base Aviano in Italien,** s. unter http://www.aviano.af.mil/Site-Pages/Article/280374/31st-communications-squadron/ **)**, und der **1st Combat Communications Squadron (von der Air Base Ramstein**, s. https://en.wikipedia.org/wiki/1st_Combat_Communications_Squadron **)** absolvierten die zweiteilige Übung. In der ersten Hälfte der Ausbildung wurden die Cyber-Spezialisten über neue Verfahren und neue Tools informiert, die bei Cyber-Analysen und zur Überwachung von Netzwerk-Aktivitäten von Nutzen sind. Die zweite Hälfte der Ausbildung diente der praktischen Erprobung der vorgestellten neuen Verfahren und Tools.

"Die bei dieser Ausbildung gesammelten Erfahrungen sind sehr wertvoll," sagte Senior Airman (Hauptgefreiter) Matthew Gorman, der für die Cyber-Verteidigung zuständige Analyst der 86th Communication Squadron. "Wir werden nicht oft zu solchen Schulungen eingeladen; deshalb war diese Gelegenheit zur aktiven Erprobung von Maßnahmen zur Cyber-Verteidigung für uns sehr wichtig."

In der zwei Wochen dauernden, unter der lateinischen Codebezeichnung "Tacet Venari" (Stille Jagd) anberaumten Übung wurden die teilnehmenden Soldaten zu Teams zusammengefasst. **Das Blue Team (in der Einsiedlerhof Air Station) hatte die Aufgabe, Cyber-Angriffe durch geeignete Verteidigungsmaßnahmen abzuwehren.**

Die Cyber-Spezialisten der 90th Cyberspace Operations Squadron auf der Joint Base San Antonio-Lackland in Texas (s. http://www.afcyber.af.mil/About-Us/Fact-Sheets/Display/Article/961989/90th-cyberspace-operations-squadron/)**, bildeten das angreifende Red Team, das die Verteidiger mit vielfältigen Cyber-Angriffen herausforderte.**

Das Blue Team verteidigte ein simuliertes Kommunikationsnetz gegen ganz unterschiedliche Versuche, in dieses Netz einzudringen oder es zu stören.

"In dieser Übung wurden die Fähigkeiten der Cyber-Spezialisten der USAFE zur Verteidigung eines Informationsraums auf eine harte Probe gestellt," erklärte Col. (Oberst) Jonathan Sutherland, der A6-Direktor und Chef der Cyber-Abwehr der USAFE. "Da wir uns noch in der Aufbauphase unserer Cyber-Abwehr befinden, haben mich die erzielten Fortschritte begeistert; in weiteren Übungen wird es darum gehen, spezielle Squadrons für die Cyber-Abwehr zu bilden."

Die Teilnehmer mussten keine Risiken eingehen, weil sie die Nutzung von Tools zur Netzwerküberwachung, die Verwundbarkeit von Netzwerk-Scannern und den Einsatz anderer Werkzeuge zu Cyber-Verteidigung in einem reinen Übungsszenario für den Ernstfall üben konnten.

"Solche Übungsszenarien sind der Schlüssel zur effektiven Ausbildung unserer Abwehr-Teams," stellte Master Sgt. Young fest. "Dabei können sie risikolos die Verteidigung gegen echte Cyber-Angriffe trainieren."

Die neuen Fähigkeiten der Cyber-Spezialisten stärken die Cyber-Abwehr der USAFE und erhöhen ihre Sicherheit.

(Wir haben den Artikel komplett übersetzt und mit Ergänzungen und Links in Klammern und Hervorhebungen versehen. Er macht wieder einmal deutlich, wie wichtig das Warrior Preparation Center in der Einsiedlerhof Air Station bei Kaiserslautern ist. Der deutschen Friedensbewegung scheint das bisher entgangen zu sei, obwohl wir seit Jahren immer wieder darauf hinweisen – was die nachfolgend verlinkten LUFTPOST-Ausgaben belegen:

http://www.luftpost-kl.de/luftpost-archiv/LP_07/LP10807_220507.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_08/LP07508_290408.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_08/LP25608_201208.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_09/LP21609_061009.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_10/LP20010_151010.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_12/LP18712_141012.pdf
http://www.luftpost-kl.de/luftpost-archiv/LP_16/LP15916_211116.pdf

Anschließend drucken wir den Originaltext ab.)

KAISERSLAUTERN AMERICAN
News for the Ramstein, Kaiserslautern, Landstuhl & Baumholder military communities in Germany

Cyber Airmen unite to protect information space

Airman 1st Class D. Blake Browning, 86th Airlift Wing Public Affairs / May 24, 2018

The U.S. Air Forces in Europe Warrior Preparation Center on Einsiedlerhof Air Station,

Germany closed the first U.S. Air Forces-Europe – Air Forces Africa cyber-only exercise on May 11.

“The purpose of the exercise was to provide training of mission defense skills and to keep our adversaries out of our information cyberspace,” said Master Sgt. Daidric Young, USAFE cyber integration manager.

Airmen assigned to the 86th Communications Squadron, 52nd Communications Squadron, 31st Communications Squadron, and the 1st Combat Communications Squadron split the exercise in two parts. The first half of the training was a cyber academic workshop teaching Airmen new procedures along with cyber analysis tools used to monitor network activity. The second half of the training was a practical application of the skills learned.

“The experience I’ve gained through this training is great,” said Senior Airman Matthew Gorman, 86th Communications Squadron cyber defense analyst. “We don’t get to practice like this too often; so we’re given this opportunity to transition from a traditional ‘comm role’ of opening and closing tickets to active cyber defense.”

The two-week-long exercise, Tacet Venari, latin for silent hunt, pooled the Airmen together forming mission defense teams (Blue Team) tasked with immobilizing adversaries through cyber defense.

90th Cyberspace Operations Squadron Airmen, located at Joint Base San Antonio-Lackland, Texas, remotely played the role as the acting adversary (Red Team) challenging the cyber defenders with a variety of attacks.

Blue team Airmen monitored and defended simulated mission essential network assets against compromise.

“This exercise was a great example of cyber Airmen sharpening their skills to better harden USAFE cyber key terrain,” said Col. Jonathan Sutherland, USAFE A6 director and chief information officer. “While we’re in the early stages of developing our cyber defense capability in theater, I’m excited about the momentum we’ve garnered; not only for future exercises, but for an eventual transition to base cyber squadrons with active cyber defense as a core mission area.”

Exercise participants were able to train on activities without risking assets, through the use of network monitoring tools, vulnerability network scanners, and other defense analysis tools, affording operators the confidence to execute in real-world scenarios.

“These training scenarios are the key to preparing our mission defense teams,” said Young. “In this environment we’re afforded real-world training without risking mission assets.”

Ensuring information is accurate, complete, and secure, mission defense teams bring new cyber capabilities to USAFE.

www.luftpost-kl.de
VISDP: Wolfgang Jung, Assenmacherstr. 28, 67659 Kaiserslautern