Spezialeinheiten überprüfen die äußere und innere Sicherheit der US-Air Base Ramstein.

LUFTPOST

Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 053/09 – 04.03.09

Angreifer-Team testet Sicherheit

Von Aaron Schoenfeld, Pressebüro des 435th Air Base Wing
KAISERSLAUTERN AMERICAN, 27.02.09
(http://www.kaiserslauternamerican.com/article.php?i=9341)

Im Ausland hängt die äußere Sicherheit vor allem von der entsprechenden Aufmerksamkeit ab. Manchmal lauert der Feind näher als wir denken.
Mit zunehmender Online-Kommunikation können Gegner Aktivitäten auf einer Militärbasis genau beobachten, ohne ihr zu nahe zu kommen. Und manchmal liefern wir ihnen sensible Informationen frei Haus.

Nach dieser unbeabsichtigten Hilfe für den Feind haben die 177th Information Warfare Aggressor Squadron (eine Einheit, welche die informationelle Kriegsführung eines Gegners imitiert) und die 57th Information Aggressor Squadron / IAS (eine Einheit, die überprüft, ob ein Gegner risikolos an wichtige Informationen kommt) vom 8. bis zum 20. Februar bei ihrem unangemeldeten Besuch in Ramstein gesucht. Das Angreifer-Team gab sich nicht zu erkennen und versuchte sich mit einer Vielzahl raffinierter Taktiken Zutritt zur Base und zu wertvollen Informationen zu verschaffen und durch harte Tests die äußeren Sicherungseinrichtungen und die Sicherung von Informationen zu knacken.

"Unser Job ist es, die Spionagetätigkeit eines Gegners zu imitieren, Aufmerksamkeit dafür zu wecken und den Leuten zu zeigen, wie man solchen Bedrohungen begegnen kann," sagte der Kommandant des 177th IAS.

Schon vor dem Besuch in Ramstein versuchte das Team durch die Auswertung offener Quellen möglichst viele Information zu sammeln. Bei diesem Verfahren geht es um das Finden, Auswählen und Auswerten öffentlich zugänglicher Quellen, die bei einer gründlichen Analyse einem Geheimdienst wertvolle Daten liefern können. An solche Informationen kommt man schon, wenn man in eine Internet-Suchmaschine "Ramstein Air Base" eingibt.

"Amerika ist eine sehr freie und offene Gesellschaft, und das ist großartig," sagte der Kommandeur des "feindlichen" Teams, "aber manchmal kann uns das auch schaden."
Weil die Verbreitung tendenziell gefährlicher Informationen nicht dadurch verhindert werden kann, dass man ganz auf das Internet verzichtet, hat das Team die zweite Woche seines Besuchs darauf verwandt, dem Personal der Base seine Erkenntnisse mitzuteilen und im beizubringen, wie potenzielle Risiken zu vermeiden sind.

Im Mittelpunkt stand dabei der sichere Umgang mit dem Internet; das Abschalten von Computersystemen, wenn sie nachts nicht gebraucht werden, das digitale Abzeichnen von E-Mails und das Verschlüsseln persönlicher Nachrichten gehören zu den Maßnahmen, die das Team empfahl, um das Netz sicherer zu machen. Seine Mitglieder ermunterten auch dazu, mit gesundem Menschenverstand auf die persönliche Sicherheit zu achten.

"Es hat sich gezeigt, dass wir (dem Gegner) hier unglaubliche Gelegenheiten bieten," sagte Col. (Oberst) Don Bacon, der Kommandeur des 435th Air Base Wing (des 435. Flugplatz-Geschwaders). "Wir haben erfahren, dass unser Netzwerk wirklich bedroht ist, und dass es Gruppen gibt, die unsere Soldaten ins Visier nehmen wollen; deshalb verstärkt dieses Training unsere Sicherheit. Das Leben und Arbeiten in einer freundlichen Umgebung hat manchmal die Wirkung, unsere Wachsamkeit einzuschläfern. Ich freue mich, dass die "Spione" uns allen einige ganz einfache Verhaltensregeln vermittelt haben, die jeder von uns anwenden kann, um unsere betriebliche Sicherheit zu verbessern."

Die Angreifer-Teams besuchen jedes Jahr mehrere Basen, und eine der am häufigsten gestellten Fragen ist, wie diese im internen Vergleich untereinander abschneiden. Das Team vergleicht zwar nicht die gefundenen Sicherheitslücken, aber die Untersucher halten fest, auf wie viele Personen sie jeweils eingewirkt haben.
Bis jetzt ist Ramstein die Base, auf der bei einem einzigen Besuch die meisten Personen geschult wurden,

"Das ist die umfangreichste Schulungsmaßnahme, die wir jemals durchgeführt haben. Wir haben unseren bisherigen Schulungsrekord um mindestens 500 Personen übertroffen," sagte der Kommandeur des Teams über diesen Besuch

Der aufgestellte Rekord sollte dafür bürgen, dass den in Ramstein arbeitenden Personen bewusster geworden ist, wie sehr ihnen ihr tägliches Verhalten schaden kann. Weil die meisten angesprochenen Methoden zur Sammlung von Daten und die Untersuchungsergebnisse über mögliche Angreifer als sensible Informationen zu betrachten sind, wurde die Ausbildung in einer abgesicherten Umgebung durchgeführt; die Ertappten waren sehr überrascht, dass man ihnen während der Untersuchung ihr Fehlverhalten wirklich nachweisen konnte.

"Wir sind nicht hier, um Leute in Schwierigkeiten zu bringen. Wir wollen dem Kommandeur der Base nur einen ersten Eindruck von den bestehenden OPSEC-Lücken und der Sicherheitssituation auf der Base vermitteln," sagte der Kommandeur des Angreifer-Teams. (Das Kürzel OPSEC steht für "Operational Security", einen Katalog, der alle äußeren und inneren Sicherheitsmaßnahmen zusammenfasst.)

"Es ist wie bei (dem jährlich durchgeführten Luftmanöver) 'Red Flag' (Rote Fahne), wenn wir uns mit den besten Piloten der 'Roten Gegenpartei' messen," sagte Col. Bacon. "Wir müssen jetzt die Taktiken und Techniken übernehmen, die uns klüger und sicherer machen."

Das Personal ist aufgefordert, auch außerhalb der Arbeit auf der Base genau darauf zu achten, was es im Internet verbreitet – in sozialen Netzwerken, Blogs und auf anderen privaten Internetseiten.

"Niemand will die Person sein, die einem Gegner das fehlende Puzzle-Teil liefert," sagte der Kommandeur (der 435th). "Bei allem, was ihr tut, müsst ihr immer davon ausgehen, dass euch jemand beobachtet. Wenn ihr euch einloggt, solltet ihr immer daran denken, dass wir im Kampf stehen."

Anmerkung des (KA-)Redakteurs: Die Namen der Angreifer wurden nicht genannt, um ihre Rolle als "feindliche Spione" nicht zu gefährden.

(Wir haben den Artikel komplett übersetzt und mit Anmerkungen und Hervorhebungen versehen. Nach unserem Kommentar drucken wir den Originaltext ab.)

Unser Kommentar

Bei seiner Suche nach Informationen und bei seinen Internet-Recherchen dürfte das Angreifer-Team auch auf unsere LUFTPOST gestoßen sein. Auch wir beziehen unsere Informationen ja ausschließlich aus allgemein zugänglichen Quellen. Wir verbreiten sie aber nicht, um irgendwelchen Geheimdiensten die Arbeit zu erleichtern. Uns geht es darum, die deutsche und zunehmend auch die europäische Öffentlichkeit über völkerrechts- und verfassungswidrige Aktivitäten der US- und NATO-Militärs in und über ihren sorgfältig abgeschirmten Anlagen auf deutschem Boden zu informieren.

Die Behauptung, das Angreifer-Team habe die Aufgabe gehabt, Ramstein besser gegen "feindliche Spione" abzusichern, ist im Zeitalter der Spionagesatelliten und der weltweiten Abhör- und Überwachungssysteme leicht als Täuschungsmanöver zu durchschauen. Es geht vor allem darum, vor den Anwohnern und einer Umgebung, die nicht mehr ganz so freundlich ist, wie Colonel Bacon behauptet, zu verbergen, was sich auf der Air Base Ramstein eigentlich abspielt. Die dort Beschäftigten sollen möglichst wenig über ihre täglichen Beiträge zu den mörderischen US-Angriffskriegen im Irak, in Afghanistan und demnächst vielleicht auch noch in Pakistan und im Iran ausplaudern, damit nicht noch mehr Einheimische auf Distanz zu "den amerikanischen Freunden" gehen und ihnen unangenehme Fragen stellen.

Die US-Basen werden zunehmend zu autarken Inseln in einer kritischer werdenden Umgebung umgebaut. Das funktioniert am reibungslosesten, wenn man alle Einheimischen zu "feindlichen Spionen" erklärt, die man sich vom Hals halten muss.

Wir werden auch weiterhin Informationen aus jedermann zugänglichen Quellen verbreiten, die das völkerrechts- und verfassungswidrige Treiben der US-Militärs und die Komplizenschaft deutscher Politiker, Juristen und Medienleute erhellen, in der Hoffnung, dass sich immer mehr Bürger/innen dagegen auflehnen.

KAISERSLAUTERN AMERICAN

Aggressor squadron tests

by Aaron Schoenfeld
435th Air Base Wing Public Affairs

In an overseas environment, physical security receives its share of due attention. Sometimes though, an enemy is lurking closer than we think.
With the increasing use of online communication, an adversary can carefully watch activity on a military base without being anywhere near it.

And sometimes, all the critical information they're looking for is handed right to them.
It's this type of unintentional assistance to the enemy that brought the 177th Information Warfare Aggressor and the 57th Information Aggressor Squadrons for an unannounced visit to Ramstein Feb. 8 to 20. The team of aggressors posed as outsiders and used a variety of advanced tactics to try and gain access to the base and valuable information through rigorous tests of physical and information security.

"Our job is to replicate an adversary's intelligence threats to raise awareness and teach people how to counter those threats," said the commander of the 177th IAS.

Prior to visiting Ramstein, the team collected as much information as possible through open source intelligence. The process includes finding, selecting and acquiring information from publicly available sources and analyzing it so it can produce actionable intelligence. Open source intelligence could be as easy to collect as typing “Ramstein Air Base” into a popular search engine.

“America is a very free and open society and that’s great,” said the “enemy” commander, “but sometimes that can work against us.”
Since avoiding the Internet altogether isn’t a viable option in preventing the dissemination of potentially harmful information, the team devoted the second week of their visit to sharing their findings and educating base personnel on how to be aware of and avoid potential vulnerabilities.

A large part of the focus was on network security. Steps such as logging off computer systems at night, digitally signing e-mails and encrypting messages with personal information are a few things that the team urges people to do to keep networks safe. They also encouraged using common sense on physical security.

“The lessons learned opportunity here is incredible,” said Col. Don Bacon, 435th Air Base Wing commander. “We know there are real threats to our networks and groups who want to target our Airmen, and this training helps us make our security stronger. Sometimes, living and working in such friendly surroundings can have the effect of letting our guard down. I’m glad they were able to come share some simple things that each of us can do to improve our operational security.”

The aggressor teams visit several bases every year and one of the most frequently asked questions is how each base fares in comparison to the others. While the team does not compare vulnerability results among bases, they do keep track of how many people they address at each location.
So far, Ramstein takes the honors for having the most Airmen educated during a single visit.

“This is the largest training venue we’ve seen yet. We were at least 500 people over our current attendance record,” said the mission commander about the visit.
The record breaking attendance provides good assurance that Ramstein personnel are more aware of how their everyday actions could work against them. And since most of the collection methods and test results of the aggressors are considered sensitive information, the training was held in a controlled environment, but surprise was obvious among those who discovered their missteps were closely tracked during the evaluation period.

“We’re not here to get people in trouble. We’re here to give the installation commander a snapshot look at the realistic OPSEC and security posture of the base,” said the squadron commander.

“It’s like flying against Red Air during Red Flag and working against the very best,” Colonel Bacon said. “Our job now is to take away the tactics and techniques that will ensure we are smarter and more secure.”

Even off base, personnel are asked to carefully consider what they put on the Internet through use of social networking sites, blogs and other personal Internet sites.

“Nobody wants to be the person that provides an adversary the missing piece of the puzzle,” the commander said. “All you need to do is always assume someone is watching.

Just consider that every time you log on – the fight's on."

(Editor's note: The names of the aggressor team members were not included to protect their roles as imitation adversaries.)

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