SOCIUS
CYBER BYTES
VOL 0.2 _ 2017

Hanging with the Hackers

By: Laura Zaroski, J.D., RPLU Socius insurance Services

This was my second year attending the DEF CON "Hackers" Conference held in Las Vegas. DEF CON has grown to over 20,000 attendees and just celebrated its 25th year. As always, it is cash only ($260) as no respectable hacker gives out his credit card number (please…).

What was "hot" this year at DEF CON? The most talked about area was the Voting Machine Hacking Village where hackers were let loose on computerized voting machines purchased by DEF CON for the conference (an exemption to the Digital Millennium Copyright Act gave the hackers a temporary pass to experiment on these voting machines). The hackers quickly discovered that the machines run on ridiculously outdated software allowing quick and easy entry into every machine, successfully manipulating the software to register fake ballots and change vote totals. Besides being disturbing, what was the point of this exercise? These results were shared with the Voting Registrars' offices making them aware of the security flaws in the hope that they will be corrected before the next election. In addition to voting machines, hackers also successfully hacked into cars, kitchen appliances and a medley of other connected devices.

Folks that hear about the conference wonder why the government does not shut it down. How can the government allow an annual conference where thousands of hackers gather to show their latest exploits? It depends on whether you look at the attendees as dangerous criminals, or gifted programmers sharing their successes. This year, Marcus Hutchins, a 23 year old British security researcher (known by his online handle - Malwaretech) was arrested by the FBI at the airport when he was leaving DEF CON. Hutchins was credited with stopping the WannaCry outbreak which likely saved thousands of companies from the Wannacry virus attack. However, the government alleges that Hutchins was involved with the creation and dissemination of the Kronos banking trojan (which attacked numerous banking institutions worldwide) and therefore, has painted him as more of a villain than hero. His fate will unfold over the next few months. So yes, attendees have been known to get in trouble at DEF CON.

Hackers generally ignore boundaries and don't conform to convention. Is this bad? Or are we just looking at them the wrong way? Are hackers criminals or patriots? Should we discourage these hackers or learn from what they can exploit? Their skills could certainly be used to protect our country from cyberattacks from foreign companies and governments (as other countries clearly have their hackers attacking the U.S.). The difference between a black hat hacker and a white hat hacker is very "grey" in my opinion. But most companies and the government don't make it easy for well-meaning hackers to productively participate in our country's cyber security. Laws like the Computer Fraud and Abuse Act make poking around inside government systems a criminal offense (and the government is generally irritated by hackers who point out their agencies' weaknesses). Further, many talented hackers are disqualified for government jobs due to the onerous background checks (as well as for the apparent requirement of short hair and collared shirts – something you don't see a lot of at DEF CON).

It is obvious that the knowledge base at DEF CON is tremendous. These talented hackers could be enormously valuable if they are properly enlisted in the fight against black hat attacks. Some companies in the private sector have already discovered the benefits of hackers. Many tech companies, such as Facebook, Apple and Microsoft now offer "bug bounty" programs, in which they offer financial rewards to hackers who find holes in their security measures. They realize that paying hackers to expose their weaknesses for a financial prize, is better than reacting to a cyber breach and the financial/public ramifications that follow. Government agencies are beginning to experiment with a similar approach, such as the Department of Defense, which offered the first-ever federal bug bounty program last year called "Hack the Pentagon".

TAKEAWAY:

Spending a weekend at Def Con is a good way to learn how all devices that are connected to the internet are vulnerable. DEF CON makes you appreciate how entrepreneurial and innovative hackers can be, as they continually push the envelope on how to use (and abuse) technology. After attending DEF CON I certainly am more cognizant of what I put on the internet, what devices I use, and how I access my own data. It also reminds me how crucial Cyber Insurance is to companies of all sizes, shapes and industries. NO ONE is immune or safe from hacking. Don't ignore the obvious threat that hacking poses to your business and bottom line. Efforts to prevent a hack are important, but as any system can be hacked, *detection and remediation* are even more crucial to the survival of any business.

Please contact your Socius broker today to discuss cyber insurance and tailoring a well drafted cyber policy to meet your clients' needs.

www.sociusinsurance.com