Did you know?

We have recently seen one of several negative consequences of not being 100% PCI compliant. ITS recently purchased a cyber breach insurance policy. There was a limitation in coverage placed on the policy with respect to fines and other damages from the banks and the card brands associated with not being PCI compliant. Unfortunately, 99% compliance is not good enough. All merchant departments much achieve 100% compliance in every way that credit cards are processed.

What’s happening on campus?
Point to Point Encryption (P2PE) Updates

Agile Ticketing Solutions is the software used by the Events Center ticketing office. Agile recently completed a software integration with Bluefin Payment Systems. We have ordered the associated credit card devices from Bluefin. Once the devices arrive on campus and are installed, the Athletics department will have PCI validated P2PE and become PCI compliant.

The Office of New Student Programs uses a software called VisualZen. Similarly, the programmers at VisualZen also recently completed an integration with Bluefin’s P2PE solution. During the orientation sessions between late May and early August, New Student Programs has a need to take numerous credit card payments in person. This summer, that will be accomplished using a Bluefin device that is integrated with VisualZen. That device is also on order from Bluefin. Although New Student Programs was already PCI compliant, P2PE will reduce their scope significantly. They will go from an SAQ C (139 individual requirements from the DSS) to an SAQ P2PE-HW (only 35 individual requirements). Also, they used to require assistance from ITS in order to take cards in person in a compliant manner. With the P2PE device, no assistance from ITS will be necessary.

Campus Recreation recently completed the RFP process for a new software. The only bidder was a company named Innosoft who provide a recreation software called Fusion. The Fusion software comes with a P2PE solution. By the time installation begins, Fusion may have two or more P2PE solution options available. Fortunately, we are seeing more and more software vendors provide P2PE with their application by entering into partnerships with P2PE solution providers.

The Parking department is in the process of acquiring new services from its current vendor, T2 Systems. Similarly, T2 will be offering a P2PE solution next quarter thanks to a partnership they entered into with a validated provider.
Compliance Issues

1. Annual Training - The training module can be found on the WeComply web site. The UCTD sent notification to everyone in early January. The UCTD will also send automated reminders monthly until the module is completed. If necessary, I will begin sending personal reminders in a month.

2. An Attestation of Compliance (AoC) is needed from your third party vendor UNLESS that company appears on the Visa Global Registry of Service Providers. In that case, please take a screen shot of the listing from the Visa web site and place it in your department’s folder on the shared drive. In the next newsletter, I will send a list of those vendors from whom we need an AoC versus those who appear on the Visa Registry.

If you have questions, please contact Steve Duseau. sduseau@binghamton.edu

Cyber-Ransom and Online Extortion - 5 Ways You Could Fall Victim

By Michael Gregg

Imagine turning on your laptop one day, only to be greeted by a bright, red screen with a warning message: “Your personal files are encrypted! ... The private key will be destroyed in 72 hours.” What would you do?

Cyber-ransom is a relatively new crime on America’s digital shores and it is spreading fast. In just the last year, the number of “ransomware” attacks have escalated globally, with one antivirus firm reporting in May that Internet users visited ransomware-infected sites 18 million times in a single six-week period!

While ransomware has actually been around for almost 10 years, until now, it’s mostly been limited to Russia and parts of Europe. But this all changed with CryptoLocker, one of the most dangerous types of ransomware that has ever been developed.

Ransomware is dangerous because it infects your computer and then encrypts all of your locally stored personal files (photos, documents, movies, music, etc.) behind a virtually unbreakable wall of encryption. The victim must pay a hefty fee to the hackers to get the files back. The FBI recently conducted a major global crackdown on the servers that were being used to host and spread CryptoLocker; however, the malware is still available for sale in the digital black market — and many other types of ransomware, new and old, are also being regularly bought and sold by cyber-criminals.

But the cyber-ransom industry is bigger than just a few crypto trojans. It’s becoming a major source of revenue and lulz for hackers around the world, most of whom are now targeting American consumers.

Here are five types of cyber-ransom attacks that could target you in the next year:

1. Ransomware
2. Hijacked Accounts
3. Sextortion
4. Denial-of-Service
5. Corporate Extortion

For more information on these attacks and how to stay safe, see the full article here: http://www.huffingtonpost.com/michael-gregg/cyber-ransom-and-online-e_b_5548810.html