What’s happening on campus?

Point to Point Encryption (P2PE) Updates

Since the last newsletter, we installed four PAX S300 credit card terminals at the Events Center ticket office. These new devices were acquired from Bluefin and are integrated with the Agile Ticketing software that Athletics uses. The installation wasn’t easy and required assistance from the networking team at ITS. But now the devices are operational and Athletics has P2PE integrated with their ticketing software. Agile just needs to make a minor change to the software that BU is running and then Athletics will have achieved compliance with the PCI DSS.

We also acquired a P2PE device from Bluefin called an ID Tech SRED Key. This device will be used by the office of New Student Programs during the upcoming orientation sessions. Currently, the device is available the remainder of the year for other uses. A few weeks ago, we tested the SRED Key in conjunction with the VisualZen software used for orientation. The device worked perfectly and was very easy to use. Not only will it reduce PCI scope for New Student Programs, but it also increases efficiency as it greatly increases the speed at which we can take in person credit card payments during orientation.

Campus Recreation and the Anderson Center continue to move forward with software changes. In both cases, the new software has an integration with a PCI validated P2PE solution. Once these merchants have their new software installed, they will also have scope reducing P2PE and have achieved PCI compliance.

In addition to the aforementioned devices, we also acquired two Nomad mobile units from Bluefin. (Pictured at right.) These hand held terminals work in conjunction with an app that runs off a smartphone or tablet. They provide quick, easy and very secure mobile payment processing. However, they do not integrate with any third party software. If any merchant department has interest in these devices, please contact Steve Duseau at Student Accounts.

Did you know?

Version 3.2 of the PCI DSS places a greater compliance burden on service providers. This may make it more difficult to obtain Attestations of Compliance from those third party vendors who process credit card payments on behalf of the university.
Compliance Issues

I. Annual Training - Out of approximately 230 employees, only 25 have not completed the training. Thank you very much to those who have. I will be in contact with those who haven’t.

II. 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. Thus far, no department has provided an AoC nor a VGR listing for 2017. Here is the breakdown by department:

1. Anderson Center: use VGR for Accesso LLC
2. Athletics: an AoC is needed from Agile Ticketing
3. Auxiliary Services: an AoC is needed from each contractor (Sodexo, B&N, etc.)
4. Campus Recreation: use the VGR for CSI Software
5. Campus Telecom: Nelnet is on the VGR, the makers of Pinnacle are not
6. Fleishman Center: PayPal is on the VGR (Sypmlicity not in use for payments)
7. Foundation: iModules and Buffalo Noel Levitz are both on the VGR
8. Graduate School: An AoC is needed from Technolutions
9. New Student Programs: An AoC is needed from VisualZen
10. Parking: T2 Systems is on the VGR
11. RF: PayPal is on the VGR (Includes Watson I/O and FBC)
12. Student Accounts: Nelnet is on the VGR
13. Student Association: An AoC is needed from University Tickets

Use of SSL/Early TLS - Vulnerability Scans May Result in FAIL by CampusGuard

Is your organization using SSL/early TLS as a security control to protect your cardholder data environment (CDE)? The PCI DSS version 3.2 states that all organizations using SSL or early TLS must be working towards a more secure version of TLS (v1.1 or higher) as quickly as possible. Note that not all implementations of TLS v1.1 are considered secure (refer to NIST SP 800-52 rev 1 for guidance on secure TLS configurations), and TLS v1.2 is highly recommended.

Per the PCI DSS, all entities must have ceased use of SSL/early TLS as a security control, and use only secure versions of the protocol after June 30, 2018. Prior to that date, any organizations with existing implementations of SSL or early versions of TLS must have a formal Risk Mitigation and Migration Plan in place. As of May 1, 2017, vulnerability scans performed by CampusGuard will result in a FAIL if a system is found to be using these insecure protocols. You will be notified of your scan results by your CRM and receive the Executive and Technical reports as per the normal process. If you have received a FAIL due to this issue, your organization will need to provide CampusGuard with a copy of your formal Risk Mitigation and Migration Plan document(s), and verify that you are working to complete the migration by the required date.

Our ASV team members will confirm receipt of the plan, and update the scan results with an exception, or False Positive, in the ASV Scan Report Executive Summary, resulting in a PASS for the scan if all other applicable scan requirements were met. If you do not have a plan in place, refer to the PCI Council's Information Supplement, Migrating from SSL and Early TLS. This guidance document outlines the information that must reviewed and provides examples of the details that should be documented within the Plan, as well as suggested migration options. You can also reach out to your CampusGuard Team for assistance with your migration plan, or if you would like the ASV team to review your documentation prior to your next scheduled vulnerability scan.