Cyber Security, Penetration Testing and Manufacturers: 10 Facts Organizations Should Know

Posted in Managed Security | Manufacturing & Distribution | Technology *on June 16, 2016*

Penetration testing is one of the most effective forms of cybersecurity for manufacturing companies. It can simulate a real-world attack and uncover areas of vulnerability within a network. As prime targets for cyber attacks, below are 10 facts about how manufacturers can gain insight and secure their systems with penetration testing.

1. Penetration testing can be performed to help all types manufacturing companies understand their information security vulnerabilities in a clear and concise manner.
2. Testing can suit your unique needs from external-facing networks and internal-facing networks to web applications, mobile applications, wireless systems or a combination of these.
3. Assessments can employ a variety of methods to identify threats, including social engineering, which is used to uncover sensitive information by email phishing attempts or calls to exploit confidential information.
4. Penetration testing can be performed to help satisfy certain compliance requirements, such as the Payment Card Industry (PCI) Data Security Standard.
5. While penetration testing is always recommended, it is a required annual activity for any entity transmitting, processing or storing 1 million or more credit card transactions with any one card brand (Visa/MC/Amex/Discover) annually, have experienced a recent PCI data breach or have otherwise been requested by a credit card processor or bank.
6. Penetration testing is also required if a company is storing credit card data in any manner, using certain kinds of desktop payment processing, online payment processing methods or acting as a PCI service provider to a third-party.
7. Testing can be utilized to help protect personally identifiable information (PII) data, such as customer and employee information and identify vulnerabilities that may expose sensitive intellectual property and trade secrets.
8. Once findings are remedied, a retesting window is important so organizations can be assured that the vulnerabilities identified are resolved.
9. Reporting is a critical component of testing. The reports generated should be written to meet the needs of an IT department, management, internal and external auditors and examiners. The reports should clearly define the scope of the testing, the methodology used and the results of the testing to make recommendations to address any findings. The reports should also be subject to a rigorous quality assurance process to ensure accuracy and completeness.
10. Penetration testing should be considered along with other closely related information security and compliance services, such as vulnerability scanning (Approved Scanning Vendor – ASV), information security consulting, on-site assessments (Qualified Security Assessor – QSA) and forensics investigations (Payments Forensics Investigator – PFI).

Cybersecurity can sometimes be an overlooked concern as some manufacturing companies have limited resources, however keeping confidential data and other sensitive information safe should be a top priority for all organizations. The value that comes from cybersecurity practices, specifically penetration testing, is taking the hypothetical to real world and learning how to protect your organization as a whole.

1

Related posts

10 Facts Not-for-Profits Should Know About Penetration Testing
Penetration testing is one of the most effective forms of cybersecurity for not-for-profit (NFP) org...

CATEGORIES

Accounting, Audit And Tax
Advisory
Agriculture
Associations
Business
Careers
Construction
ERP & CRM Software
Government
Healthcare
Higher Education
Leadership
Managed Services
Manufacturing & Distribution
Manufacturing Jobs
Metal Fabrication
Not-For-Profit
Oilfield Services
Professional Services
Real Estate
Retail
Tech Tips
Technology