DCU BULLETIN

Division of Credit Unions

Washington State Department of Financial Institutions

Phone: (360) 902-8701 ***FAX: (877) 330-6870***

September 25, 2019 No. B-19-05

Free Cybersecurity Resources
Department of Homeland Security's
National Cybersecurity Assessments and Technical Services (NCATS)

Introduction

The Division of Credit Unions' examination focus for 2019 highlighted cybersecurity risks as a continued area of concern. The National Association of State Credit Union Supervisors (NASCUS) held a webinar to share information about several **no cost** resources available from the Department of Homeland Security's NCATS Division. These resources are available to credit unions of all sizes to assess and improve their cybersecurity posture and identify operational strengths and weaknesses.

The following is a list of service currently available:

Vulnerability Scanning (Cyber Hygiene)

- Scanning of Internet accessible systems for vulnerabilities on a near continuous basis.
- Customers receive weekly reports that include current scan results, historic trends, and result comparisons to the national average.

Phishing Campaign Assessments

- Measure an organization's propensity to click on email phishing lures.
- Assessment results can be used to provide guidance and justify resources to defend against spear-phishing and increase user training and awareness.

Reputation and Posture Monitoring

- Scanning of Internet accessible systems to identify possible configuration errors and suboptimal security practices.
- Monitoring of dark-web sites, social media platforms, and other data sources for attack precursors, indicators of systems or account compromise, excessive organizational information, and signs of data leakage of exfiltration.

Risk and Vulnerability Assessments

- One-on-one engagements with customers that combine national threat and vulnerability information with data collected and discovered through onsite assessment activities.
- Risk analysis reports with actionable remediation recommendations prioritized by risk.
- Service components include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration management reviews of servers and databases, and operational response maturity evaluation.

Remote Penetration Testing

- Assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Emphasis on rapid identification and elimination of vulnerabilities and attack paths prior to this exploitation by a malicious actor.
- Focus only on externally accessible systems.
- Ideal for testing centralized data repositories and assets accessible online.

Validated Architecture Design Review

- Evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner.
- Includes design architecture review, systems configuration and log file review, and analysis of network traffic.
- An in-depth report including key discoveries and practical recommendations for improving an organization’s operational maturity and enhancing their cybersecurity posture is provided.
- Designed for OT and IT networks.

Conclusion

If you have any questions about the NCCIC, would like more information on what services are available, or would like to request services, contact ncciccustomerservice@hq.dhs.gov or 888-282-0870.

If you have any questions about this Bulletin, please contact Tammie Nuber at Tammie.Nuber@dfi.wa.gov or (360) 902-8717.