ASPR TRACIE Technical Assistance Request

Requestor: [redacted]
Requestor Phone: [redacted]
Requestor Email:
Request Receipt Date (by ASPR TRACIE): 12 January 2017
Response Date: 19 January 2017
Type of TA Request: Standard

Request:

[redacted] asked if ASPR TRACIE had example After Action Reports/ Improvement Plans (AARs/ IPs) on ransomware attacks on a small hospital.

Response:

The ASPR TRACIE team reviewed existing Topic Collections for materials on ransomware and AARs/ IPs; namely, the Cybersecurity and Exercise Program Topic Collections. We also searched for other resources online but were unable to find specific AARs/ IPs related to hospital ransomware incidents. However, in Section I below, we provide a resource that includes several AARs from an annual U.S. Department of Homeland Security exercise. Section II includes multiple resources on lessons learned from ransomware attacks, which we believe will be helpful to your request. Finally, Section III includes other resources related to ransomware and healthcare, to include cyber tabletop exercise materials.

I. Ransomware After Action Reports

U.S. Department of Homeland Security. (2016). Cyber Storm: Securing Cyber Space.

> Cyber Storm is the U.S. Department of Homeland Security's biennial cybersecurity exercise. This webpage includes highlights and lessons learned from exercises and links for more information. Note: The final reports for all Cyber Storm exercises can also be located here: https://www.dhs.gov/publication/cyber-storm-final-reports.

II. Lessons Learned from Ransomware Attacks

ASPR TRACIE. (2016). Cybersecurity and Healthcare Facilities. U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response.

> Cybersecurity is a critical issue facing the ASPR TRACIE audience. In this webinar, a distinguished panel of experts describe lessons learned from recent experiences, planning considerations, and steps the federal government is taking to address cybersecurity and cyber hygiene.

ASPR TRACIE. (2016). The Exchange, Issue 2. U.S. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response.

This issue of the ASPR TRACIE newsletter focuses on cybersecurity and cyber hygiene.

Davis, J. (2016). Human Element the Weakest Link in Healthcare Security, Says Verizon Report. Healthcare IT News.

Verizon examined more than 100,000 security incidents and found that of the 166 healthcare breaches, 115 had confirmed data loss, 32% were caused by stolen assets, and 23% were a result of privilege misuse. The report also found reuse of credentials to be a healthcare-specific risk.

Duncan, I., McDaniels, A.K., and Campbell, C. (2016). Hackers Offering Bulk Discount to Unlock Encrypted MedStar Data. The Baltimore Sun.

The authors provide an overview of a recent attack on MedStar (a system in the Baltimore-Washington, DC region), highlighting the need for newer employees to also be familiar with more traditional (non-electronic) paper-pencil methods for maintaining records.

Stone, J. (2016). (2016). Hackers Ransom Attack on California Hospital More Proof Healthcare Cybersecurity Is Floundering. International Business Times.

The author provides an overview of the cyberattack on Hollywood Presbyterian Medical Center (CA).

Verizon. (2016). 2016 Data Breach Investigations Report.

This comprehensive report details data from over 100,000 incidents affecting various industries, including healthcare. Victim demographics, vulnerabilities, phishing, and incident classification patterns are discussed and an entire appendix is devoted to "attack graphs."

III. Other Ransomware-Related Resources

Callahan, M. (2016). What Hospitals Need to Know about Ransomware. American Hospital Association.

The author provides a brief introduction and overview of ransomware, how it can be used to infect mobile and desktop devices, and the importance of security and regularly backing up patient and facility data.

Shaghaghi, S. and Pilch, P. (2016). HIT Think Ransomware: What Providers Should do now. (Registration required to access entire article.) Health Data Management.

The authors discuss steps facilities can take to prevent and mitigate the effects of a ransomware attack.

Shaghaghi, S. and Pilch, P. (2016). Preparing For and Responding To Hospital Ransomware Attacks. BDO.

The authors illustrate the actual and projected rise of ransomware attacks on all industries, and share related preparedness and response strategies for healthcare facilities.

United States Computer Emergency Readiness Team. (2016). Ransomware and Recent Variants.

This factsheet provides an overview of ransomware and shares how the variants Locky and Samas were recently used to compromise healthcare networks.

U.S. Department of Health and Human Services. (2016). How to Protect Your Networks from Ransomware: A Letter from HHS Secretary Burwell.

This letter from HHS Secretary Burwell provides information on the increasing threat of ransomware to the healthcare industry. It also includes materials on how to protect networks from such threats.

U.S. Department of Homeland Security. (2013). DHS Cyber Tabletop Exercise (TTX) for the Healthcare Industry.

This package of materials can help healthcare industry organizations plan and organize a cyber tabletop exercise.