November 2017

NCDPI Cybersecurity Newsletter

Welcome to the second NCDPI Cybersecurity newsletter in our series of communications. For those seeing this for the first time, my name is KC Hunt and I am the department's Information Security Officer. This newsletter provides you the opportunity to ask questions and receive answers regarding cybersecurity and how it impacts your life. Please email me any suggestions on issues you would like covered, and I will provide you with information that should make your lives (professionally and personally) more secure.

The Dark Overlord:

The education community has been a target for extortionists for the last couple of months. A group calling themselves "The Dark Overlord" has stolen data from schools in four states (Iowa, Montana, Texas, and Alabama). The group gains access to student data, steals it and then uses the data to blackmail the school districts. They email, text, and threaten to post sensitive data (IEPs, counseling records, grades, student and parent contact numbers, etc.) unless the school pays them in bitcoin. On Oct 4, 2017, the group claimed responsibility in Iowa and dumped stolen data on Pastebin with the note "The better to help child predators." The going rate as of the last ransom note was $150K. This ties into the note about patching below. The systems need to be patched to make it harder for the bad guys to exploit a system.

Security in vendor cloud systems

As IT professionals, you may want to ask your vendors questions about the cloud hosting solution that you are considering, or already have a contract. With all the recent news, it seems like cloud systems do not provide the security they advertised. Recently Verizon, National Geo-Spatial Intelligence Agency (NGA), Deloitte, and North Carolina-based security firm TigerSwan have all had their Amazon hosted servers compromised due to poor configuration and patching solutions. In some ways, cloud solutions are good, but only if the **owner** of the hosted system understands the security provided by the cloud and their responsibilities to their customers.

There is a very good video recorded by a technical evangelist at Amazon Web Services (AWS). It is a one-hour video, and probably more than you want to know, but Ian Messingham does a very thorough job explaining how security works with AWS. AWS takes no responsibility for the secure configuration of the operating system or security monitoring, application security configuration or monitoring, account management, access control lists, or identity management among other things. Amazon provides great tools for

implementing security controls, but as you'll see in this Amazon video (44 minutes), you need to be very skilled to deploy them broadly and effectively

Patching

I know what you are thinking. Patching sounds like a broken record among security people.

One of the highlights that came out of the 2016 cyber security survey was that patch management was identified as needing attention. Both the policy side and the implementation side were identified as having shortcomings. The importance of patching systems cannot be over emphasized. If you follow the news and/or the security letters, you can read about companies (SEC, Equifax, Sony) that have been compromised and the root cause was failure to patch. When you read the detailed "after action report" on the breaches you start to understand that while phishing emails, or other social engineering techniques are often the first encounter, the systems that were compromised were missing patches, which allowed the bad guys to exploit the system, steal data and move around the environment looking for more lucrative data to steal or encrypt for ransom. The NC State Information Security Manual has a section on patching and recommended timeframes.

Vulnerability Mitigation

Mitigation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Rating as provided by a vulnerability scan or risk assessment.

- "Critical-level risk" vulnerabilities must be mitigated as soon as possible. "Critical-level risk" vulnerabilities must be, at a minimum, mitigated within seven days, and remediated (if possible) within 21 days.
- "High-level risk" vulnerabilities must be mitigated or remediated within 30 days.
- "Medium-level risk" vulnerabilities must be mitigated or remediated within 60 days.
- "Low-level risk" vulnerabilities must be mitigated or remediated within 90 days.

Following is a policy that you may want to use as a template to get started. If you see something that can be improved, please let me know. We are all in this together.

Please feel free to suggest topics that you would like addressed in upcoming newsletters by contacting me at kc.hunt@dpi.nc.gov or (919) 807 4068.

Public Schools of North Carolina
State Board of Education
Department of Public Instruction

Stay Connected with North Carolina Public Schools: