Del Rio NEWS-HERALD

January 18, 2019

Cyber attack on City Hall, an ongoing trend

By Rubén Cantú

Dr. Wesley McGrew, Director of Cyber Operations at Horne Cyber, a cyber security firm.
Contributed photo

The cyber attack affecting the city of Del Rio's computer systems is part of a trend targeting specific information that could represent liability, such as emails and financial data, a cyber security expert said Thursday.

Dr. Wesley McGrew, Director of Cyber Operations at Horne Cyber, a cyber security firm with offices in Washington D.C., Mississippi, and Tennessee, said experts are currently seeing a rise in extortion-based attacks.

The city of Del Rio reported a ransomware attack forced its IT department to shut down the city’s servers on January 10.

McGrew said the number of attacks occurring in the U.S. is nearly uncountable, as everyone from an individual to government agencies and services are the targets of these attacks.

“At any given time there are a few ‘campaigns’ of ransomware that are prevalent and share common attribution in terms of who’s spreading them and/or authoring the ransomware software,” McGrew said in an email.

The victims each day of the widespread campaigns number in the thousands, and that’s not counting smaller, upcoming, or developing campaigns, he said.

McGrew said small communities and city governments are no strangers to ransomware attacks.

“I would venture to guess that there is no city government that ‘hasn’t’ been the target of one of these campaigns. We have performed incident response investigations into successful attacks on municipalities, and it’s my assessment that ransomware operators are specifically targeting local and state governments,” he said.

According to the cyber security expert, most ransomware incidents begin with attacks on un-patched systems, or accounts with poorly chosen passwords (common words, or using the same password as disclosed in another breach).

Ransomware attacks, he said, have a particularly high impact on business networks where individual users have broad access to lots of critical data, such as on a shared network drive.

The best way to help prevent these attacks, he said, is to keep systems patched and up-to-date, enforcing a strong password policy, and moving to a two-factor authentication.

“There will always be new avenues, though, so a careful examination of user privileges and internal network security is important,” he said.

“A penetration test can help find issues that policy reviews miss,” he said.

Horne Cyber, he said, developed a software to provide IT staff with a tool for looking at how a ransomware campaign might spread across a network due to a single vulnerability or user compromise.

During a typical ransomware attack, he said, data is encrypted in-place, while the operator of the ransomware is the only one with the key.

“In cases like that, there is no exposure to the data – exactly the opposite: nobody can access it. We are seeing a rise in extortion-based attacks, though, which may mean that ransomware operators may specifically seek data that is embarrassing or represents a liability, such as email and financial data,” he said.

Horne Cyber’s flagship service is advanced penetration testing. They use teams of specialists trained to operate like real hackers to find vulnerabilities in their clients’ networks while recommending remediation.

The cyber-attack targeting the city of Del Rio affected services provided to the public, including limiting bill payments to checks and cash only.

Del Rio News-Herald

...