EDMOND Life & Leisure

Edmond Life & Leisure • 107 S. Broadway • Edmond • OK • 73034 • Phone: 405-340-3311

Ransomware threat is more prevalent

Thu, Sep 28, 2017

By Lane Griffing

Information technology professionals have seen numerous changes affect Oklahoma businesses over the past 15 years. However, new threats have emerged which are capable of indiscriminate and devastating damage to business information.

One of the most prevalent threats is a type of malicious software known as ransomware. Rather than directly steal data, ransomware steals an organization's access to data by encrypting information that is shared on the network. Typically the only means to regain access to the data is to restore from backups.

The reason why this type of attack has received so much attention is that it has disrupted numerous successful businesses. These are businesses who have the professional resources to secure their data properly. Even with their resources they have had data damaged and in some cases have paid tens of thousands of dollars to regain access. If there is a lesson in this, it is that ransomware can affect any business regardless of size. Ransomware is being aggressively improved upon, upgraded and implemented. This results in an increasing requirement to make security adjustments in order to remain compliant with best practices and reduce ransomware risk.

The reason why this threat has become so prevalent is because it is highly profitable. The FBI has estimated that over $1 billion in ransom payments were made in 2016, and Trustwave Global Security Report estimates that ransomware has yielded over 1,000 percent profit for some perpetrators.

According to antivirus vendor Trend Micro, 80 new ransomware families emerged in the same year with over 30,000 variants. Due to the fact that ransomware development kits are available online it is reasonable to expect the variety of this malware to grow. Although the techniques used to avoid infection are not necessarily difficult, it does involve both technical and personnel training solutions.

Since the most prevalent means of infection is via phishing e-mails, detailed attention to antispam and email system configuration is required, as well as user training on recognition of phishing emails. Phishing emails are designed to convince the user to either click a dangerous link or open an innocent-looking attachment to initiate the infection. Proper configuration and tuning of antivirus systems is necessary to detect ransomware behavior and to halt the infection process. Having appropriate protection from both onsite and offsite backups can reduce the impact of successful ransomware attacks.

To appreciate the critical importance of backup and disaster recovery, it is necessary to imagine that a ransomware attack has occurred and that most business data has been encrypted and is now unusable. Paying a ransom does not solve the issue, because receiving a working decryption key is unlikely. The only feasible option is to recover data from a backup. If backups of all business data are run on an hourly basis and the ability to recover is tested and documented then recovery is relatively painless. Businesses should ascertain the location of all critical data, including e-mail, and verify that it is being backed up, and that recovery is being tested. We also recommend that businesses evaluate their disaster recovery design, and run periodic drills to validate and adjust these procedures.

Google

WEEKLY HIGHLIGHTS

Local News
- St. Augustine's Arts & Crafts Faire nears
- Edmond to celebrate Halloween on Oct. 31
- 'One Gift Serves Many'
- Edmond Elks Lodge part of Kids Fishing Derby
- 'Power of Children' exhibit continues through Oct. 20

Sports News
- UCO Alumnus Chad Richison Gifts $4 Million to 'Complete the Dream'
- OC will take up bowling
- Bronchos' last ditch pass comes up short

Business News
- Ransomware threat is more prevalent
- Dealing with aftermath of Equifax's hacking
- New Edmond area mortgage lender
- Leadership Edmond class is selected by Chamber
- Joins staff of OU Physicians
- Energy companies help with relief effort
- Abstract company featured in the EEDA's newsletter

Education News
- Ex-Gov. Keating will team up with Lincoln
- Four State titles in a row for North Cheer team
- Alumni Association awards scholarships

Entertainment
- 'Tosca' opera will open next month

Health and Fitness News
- Concordia Partners with St. Mark Lutheran Church to Offer Free Wellness Clinic
- Health professionals join McBride

Miscellaneous News
- Pet blessing on Oct. 7
- The do's & don'ts of do-it-yourself
- Renters insurance & the many myths

At the Movies with George
- Sleeper hit of the year

VIRTUAL EDITION:

View this week's paper online!

Having excellent documentation of both existing information systems and of the procedures used to protect them is a key component of successful disaster recovery. The information required goes much deeper than network maps and procedures, but includes a triage plan with system recovery already prioritized, drivers, spare hardware, network isolation procedures, and a host of other information.

This preparation varies by business and by the business systems in use. If businesses invest the effort before they experience an attack, the likelihood of a good outcome is substantially improved.

At Dolce Vita IT Solutions, we have experienced that a significant challenge is getting management teams to invest time in recurring user training. For the past 18 months, we have provided free training to our clients … and this has proven its worth in that out of the last 34 documented ransomware attacks against our clients, the users defeated 33 of those attacks. The only seriously damaging attack occurred with a client who declined training. This attack resulted in severe damage to two of the client's servers, resulting in them being restored from backups. Following this attack the client allowed us to train their users which resulted in the users defeating a later ransomware attack. Although technology deals with 50-75 percent of the threat, users continue to be the last line of defense. We recommend that ownership and senior management teams provide their users with the tools and skills to protect their business. About the author: Dolce Vita IT Solutions (*www.dvits.net*) is an Edmond, Oklahoma based IT consulting firm specializing in providing IT support to small and mid-sized businesses in medical, insurance, manufacturing, banking, and other business verticals. In business since 2002, Dolce Vita works with businesses from 2 to 500 users. Lane can be reached at *lane.griffing@dvits.net*.

A graduate of the University of Oklahoma, Lane has nearly 15 years of oil and gas experience and over 15 years of information technology experience. His initial communications experience was as a communications platoon commander with Third Battalion, Eight Marines, and as a technical communications evaluator for the Second Marine Expeditionary Force Special Operations Training Group. His business focus with Dolce Vita IT Solutions is on strategic IT planning, disaster recovery design, and automated network management.

View At Home Summer 2017

View Calendar of Events 2017

NEWS:

Cover Stories
Local News
Sports News
Business News
Education News
Spotlight On Seniors
Entertainment
Political
Health and Fitness News
Miscellaneous News

COLUMNS:

From The Publisher
Steve Gust
Governer Mary Fallin
At the Movies with George
Susan Henry Clark
Dave Farris
Opinion

Letter to the Editor

Edmond Family Counseling

Business of the Week

What's Happening This Weekend

SOCIAL MEDIA: