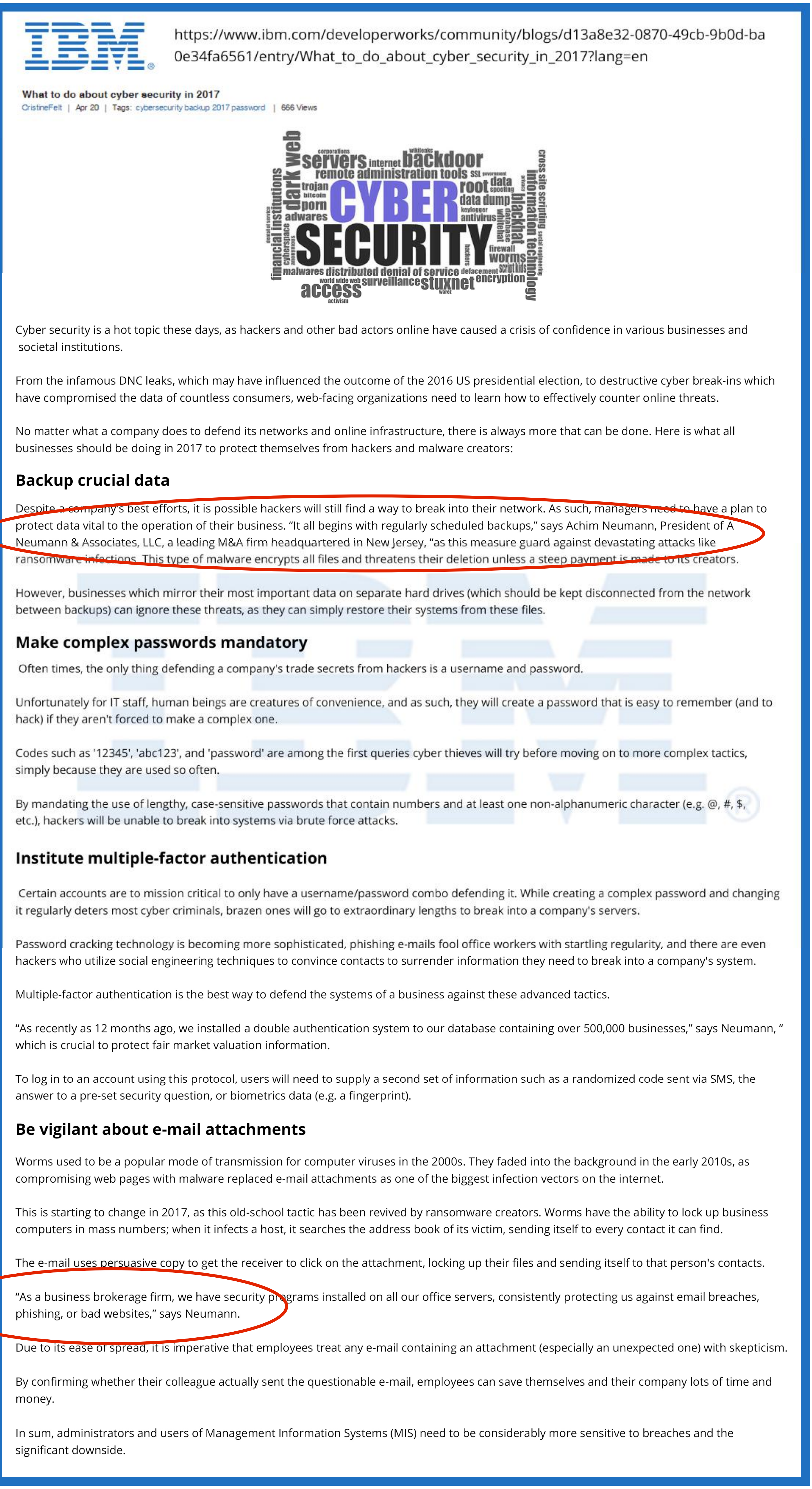

https://www.ibm.com/developerworks/community/blogs/d13a8e32-0870-49cb-9b0d-ba0e34fa6561/entry/What_to_do_about_cyber_security_in_2017?lang=en

What to do about cyber security in 2017

CristineFelt | Apr 20 | Tags: cybersecurity backup 2017 password | 666 Views

Cyber security is a hot topic these days, as hackers and other bad actors online have caused a crisis of confidence in various businesses and societal institutions.

From the infamous DNC leaks, which may have influenced the outcome of the 2016 US presidential election, to destructive cyber break-ins which have compromised the data of countless consumers, web-facing organizations need to learn how to effectively counter online threats.

No matter what a company does to defend its networks and online infrastructure, there is always more that can be done. Here is what all businesses should be doing in 2017 to protect themselves from hackers and malware creators:

Backup crucial data

Despite a company's best efforts, it is possible hackers will still find a way to break into their network. As such, managers need to have a plan to protect data vital to the operation of their business. “It all begins with regularly scheduled backups,” says Achim Neumann, President of A Neumann & Associates, LLC, a leading M&A firm headquartered in New Jersey, “as this measure guard against devastating attacks like ransomware infections. This type of malware encrypts all files and threatens their deletion unless a steep payment is made to its creators.

However, businesses which mirror their most important data on separate hard drives (which should be kept disconnected from the network between backups) can ignore these threats, as they can simply restore their systems from these files.

Make complex passwords mandatory

Often times, the only thing defending a company's trade secrets from hackers is a username and password.

Unfortunately for IT staff, human beings are creatures of convenience, and as such, they will create a password that is easy to remember (and to hack) if they aren't forced to make a complex one.

Codes such as '12345', 'abc123', and 'password' are among the first queries cyber thieves will try before moving on to more complex tactics, simply because they are used so often.

By mandating the use of lengthy, case-sensitive passwords that contain numbers and at least one non-alphanumeric character (e.g. @, #, $, etc.), hackers will be unable to break into systems via brute force attacks.

Institute multiple-factor authentication

Certain accounts are to mission critical to only have a username/password combo defending it. While creating a complex password and changing it regularly deters most cyber criminals, brazen ones will go to extraordinary lengths to break into a company's servers.

Password cracking technology is becoming more sophisticated, phishing e-mails fool office workers with startling regularity, and there are even hackers who utilize social engineering techniques to convince contacts to surrender information they need to break into a company's system.

Multiple-factor authentication is the best way to defend the systems of a business against these advanced tactics.

“As recently as 12 months ago, we installed a double authentication system to our database containing over 500,000 businesses,” says Neumann, “ which is crucial to protect fair market valuation information.

To log in to an account using this protocol, users will need to supply a second set of information such as a randomized code sent via SMS, the answer to a pre-set security question, or biometrics data (e.g. a fingerprint).

Be vigilant about e-mail attachments

Worms used to be a popular mode of transmission for computer viruses in the 2000s. They faded into the background in the early 2010s, as compromising web pages with malware replaced e-mail attachments as one of the biggest infection vectors on the internet.

This is starting to change in 2017, as this old-school tactic has been revived by ransomware creators. Worms have the ability to lock up business computers in mass numbers; when it infects a host, it searches the address book of its victim, sending itself to every contact it can find.

The e-mail uses persuasive copy to get the receiver to click on the attachment, locking up their files and sending itself to that person's contacts.

“As a business brokerage firm, we have security programs installed on all our office servers, consistently protecting us against email breaches, phishing, or bad websites,” says Neumann.

Due to its ease of spread, it is imperative that employees treat any e-mail containing an attachment (especially an unexpected one) with skepticism.

By confirming whether their colleague actually sent the questionable e-mail, employees can save themselves and their company lots of time and money.

In sum, administrators and users of Management Information Systems (MIS) need to be considerably more sensitive to breaches and the significant downside.