Cyber Crime Damage Costs to Exceed 6 Trillion by 2021

Steve Reich March 13, 2018

Cyber security is not just an IT issue; itâ€™s an organization issue

Forty-three percent of cyber attacks target small businesses. Sixty percent of small companies go out of business within six months of a cyber attack.

(Newswire.net -- March 13, 2018) Clearfield, Utah -- With new firewall technology, preventing Cyber-crime is no longer a Mission Impossible. Cyber-attacks are coming at businesses from every direction on a daily basis. Although often considered a society problem, at the end of the day, the financial consequences of a breach fall on the shoulders of the company executives. These losses could be any of the following: actual dollars lost, customers trust loss or short or long-term brand damage. All of these are long-lasting and often devastating hits to companies in our economy.

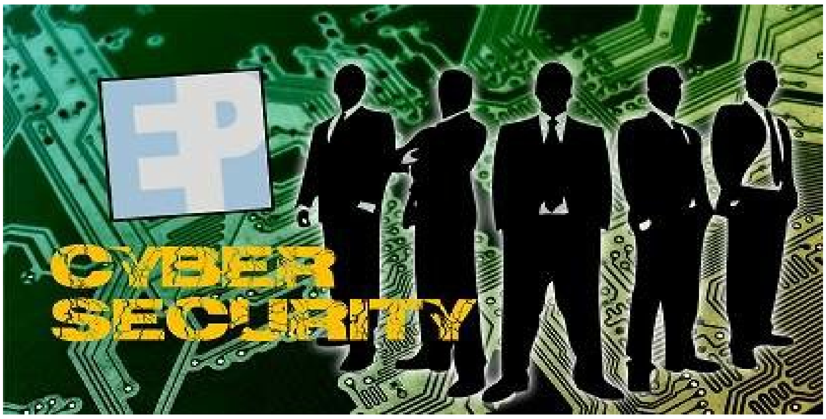
The traditional approach to cyber-crime prevention was to add more layers of security. The approach was to build up the fortress; adding anti-virus protection, more expensive firewalls, including any other existing blacklist technology. Once our reactive fortress was built we would then cross our fingers, hoping our overworked IT staff would catch any breaches before too much damage is done.

Robert Abram, CTO of EntPack, a cyber security company based in Utah, likened this traditional approach to a casino. He said, *“As long as you aren’t on the bad list, you are welcome to come in and play. But as soon as you do something that hurts the casino, you’re out and added to the list of people who aren’t allowed to come back to the casino. But, nothing was put into place to proactively stop the initial loss and there’s nothing stopping you from disguising yourself and trying to play again the next day.”*

This type of cat and mouse game seems like a losing battle, or at least an expensive one to play. It’s no wonder cyber-crime damage costs are expected to hit $6 trillion annually by 2021. (data according to Cybersecurity Ventures) Once infamous security breaches as in Wannacry and Petya were **blacklisted,** the cyber-criminals just started working on other approaches. Today, we cannot afford to only be reactive, the cyber criminals who were not caught, gained knowledge and experience from these previous strains and so their next attempts will likely be stronger and more robust.

Our research shows that Abram’s company, EntPack, has developed a process with technology that is a **proactive** approach to avoiding cyber-crime. EntPack’s flagship firewall, Sandtrap, marries advanced blacklist technology with a host-filtering approach to mitigate risk. User reports identify this firewall product of being both extra-secure all while being easy-to-use and network-administrator-friendly. The Sandtrap has been specifically designed for ease of use. *“It makes good financial sense to use good host-filtering technology at the firewall layer in your defenses,”* Abram said.

Blacklist-only thinking is truly a reactive strategy. In order for the blacklist technology to stay current, someone has to be victimized. Now, we all understand that there are casualties in war, but if you can avoid being the victim wouldn’t you do it? So why then do we keep focusing on the same type of technology and keep our fingers crossed that the next malware strain will be discovered on someone else’s network?



“A focus solely on blacklist technologies is a risky approach to securing your data,” Abram said. *“If there’s a dinner party at the White House and you aren’t on the guest list, then you aren’t getting into that party. And they aren’t going to stand around and let you keeping trying to get through the front door.* ***Host filtering****, or sometimes called “****whitelisting****,” is a more secure option.”*

Phishing attacks are a huge problem because they target your employees. A blacklist approach will keep known threats out of their inboxes, but new threats are allowed to pass through your defenses. These malicious emails often trick good employees into clicking on malicious links and thereby providing the attacker with access to your network. A strong host filtering engine can help mitigate these types of attacks.

The Sandtrap’s host filtering engine works on a scale never seen in any firewall product before. While most firewalls can filter hosts in the thousands without experiencing slowing, the Sandtrap can filter in the millions. Setting rules and creating policies for individual users or systems is simplified through this firewall. Gone are the days when a company needs to pay six full-time employees to manage their whitelist. Using Sandtrap and one or two employees; your network can be more secure. Those four or five extra IT employees can now go back to helping employees with their other software and hardware issues.

Technology and process advancement allows companies today to be able to take a proactive stand against the growing cyber-fraud disease. No more living in a reactive-only world as an approach to cyber security.

About EntPack

<Please fill out "Company Description">

EntPack

1412 S. Legend Hills Dr.
Clearfield, Utah 84015
United States
1-866-224-5744
elizabeth.abram@entpack.com
http://www.entpack.com
Source: http://newswire.net/newsroom/pr/00100652-cyber-crime-damage-costs-to-exceed-6-trillion-by-2021.html