The Threat is Real

completecloud
POWERED BY AVATARA

5 days ago - Hackers have infected every public computer in the St. Louis Public Library system, stopping all ... St. Louis' public library computers hacked for ransom ... a particularly nasty type of computer virus that encrypts computer files.

4,000 ransomware attacks per day in 2016.

Ransomware: malicious software that will prevent the user access until a sum of money is paid.

- It's the fastest growing malware threat and these attacks are typically automated and target anyone and everyone. They can also leak victim's information until the ransom is paid. Joseph Bonvalonta, a Special Agent in the FYI Cyber Intelligence, said, "Ransomware is that good...To be honest, we often advise people just to pay the ransom."

Phishing is now the #1 delivery vehicle for ransomware and other malware (Verizon 2016 DBIR).

"...the email was a phishing attack....The blunder gave Kremlin hackers access to about 60,000 emails in John Podesta's private Gmail account."

Phishing: fraudulent emails that are designed to trick employees and individuals to reveal personal information ranging from passwords to credit cards.

- These emails are becoming extremely sophisticated and can be challenging to determine if it is actually legitimate email or a phishing attempt. They can come from sites that you frequent and emails you are used to seeing, such as Amazon confirmations or survey requests. The Democratic National Committee was hacked through these phishing emails which simply read, "Someone just used your password to try and sign into your Google account. Click here to Change password."

Sony Picture's hack "erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers."

In 2015 the medical and healthcare industry experienced 276 security breaches, exposing over 121 million records; while 63 security breaches involving the government or the military exposed the records of 34 million individuals.

Hacker: an individual that gains unauthorized access to computer systems to obtain information, normally with malicious intent.

- Hackers can easily obtain access to a company's system when proper security measures aren't taken. They can reside in a system for months, going completely undetected and exploiting whatever they see fit. Not taking advantage of proactive cyber security measures will end up costing companies more time and money in the long run. Hewlet Packard reported that a hack can costs the average American firm $15.4 million.

Compliance Ramp Up

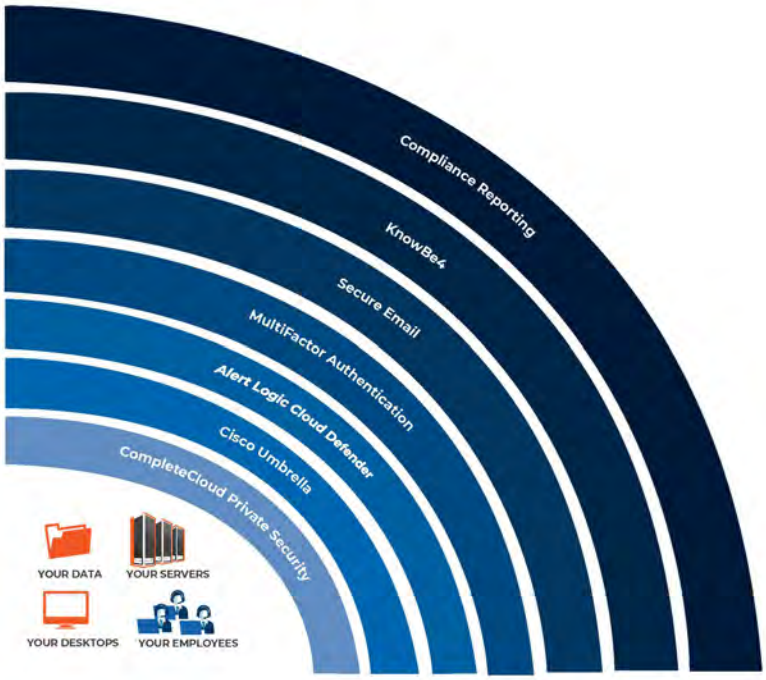
The National Institute of Standards and Technology (NIST) is a small agency that develops the standards, processes, and cyber security practices for all government agencies and various other industries. NIST recently raised their standard for cyber security and reporting, which affects a lot of organizations. Two major players that have been affected by this are Defense Federal Acquisition Regulation Supplement (DFARS) and the Health Insurance Portability and Accountability Act (HIPAA), since they are dealing with highly classified military contracts for the government and personal patient information. Any company or healthcare organization that deals with DFARS or HIPPA has been scrambling to find a way to meet the security standards their industry now demands.

AT&T Partner Exchange®
Platinum Solution Provider

https://www.fidelitech.net | 801-263-8858 | 2130 South 3140 West, Suite A, Salt Lake City, Utah 84119

The Threat is Real

completecloud
POWERED BY AVATARA



CompleteCloud utilizes a 24/7 Security Operations Center and some of the biggest names in cyber security, like Cisco Umbrella and Alert Logic, to help reduce the chances of your business being affected by malware. If you're concerned about meeting industry standards like HIPAA or Sarbanes-Oxley, you're covered. We will provide the reports to show your auditors that your systems are secure. CompleteCloud allows you to operate with the peace of mind that your business is safe, data secure, and industry standards meet regardless of the cyber threat.

Private Cloud

With CompleteCloud all your data gets transitioned into the data centers, which will remove the opportunity for bots to enter your company's infrastructure by getting rid of any unneeded open ports. Server and edge firewalls, along with intrusion detection software, help to continually protect your data.

Cisco Umbrella

Predictive cloud based security that leverages the internet to take in millions of data points per second to identify suspected threat origins. Not only does Cisco Umbrella block threats and run analytics, but it is completely automated and always searching. Cisco Umbrella prevents malware and blocks phishing attempts and inappropriate content, while containing any botnets.

Multi Factor Authentication

Helps provide additional security for remote user logins so when a laptop is lost, or left unattended with a sticky note on it that just so happens to have the username and password, no one but you can get in. In addition to a user login there is a quick cell phone call to substantiate your identity is correct and will then grant you access.

Alert Logic Cloud Defender

Alert Logic continually monitors network traffic for any unknown threats and analyzes all the data it collects to better identify potential risks later on. These non-stop assessments help find and identify any vulnerabilities and exposures that your system may have which will allow you to rest assured your information is protected. All of this is coupled with Alert Logic's Security Operations Center (SOC) that provides 24/7 monitoring by GIAC-certified analysts. This level of security and threat analysis helps meet rigorous PCI DSS, HIPAA, and Sarbanes-Oxley requirements.

KnowBe4

KnowBe4 is the world's largest security awareness training and simulated phishing platform. KnowBe4 is designed to teach employees how to avoid social engineering through training and real world examples and application.

Secure Email

Secure Email is an email management software that allows you to archive search emails, increase email security policies and limits, and send encrypted emails.

Compliance Reporting

CompleteCloud also provides quarterly comprehensive compliance reports to your customers, regulators, or auditors so they can sufficiently inspect your infrastructure. Regardless if you're getting assessed by HIPAA or DFARS, you're covered.

https://www.fidelitech.net | 801-263-8858 | 2130 South 3140 West, Suite A, Salt Lake City, Utah 84119