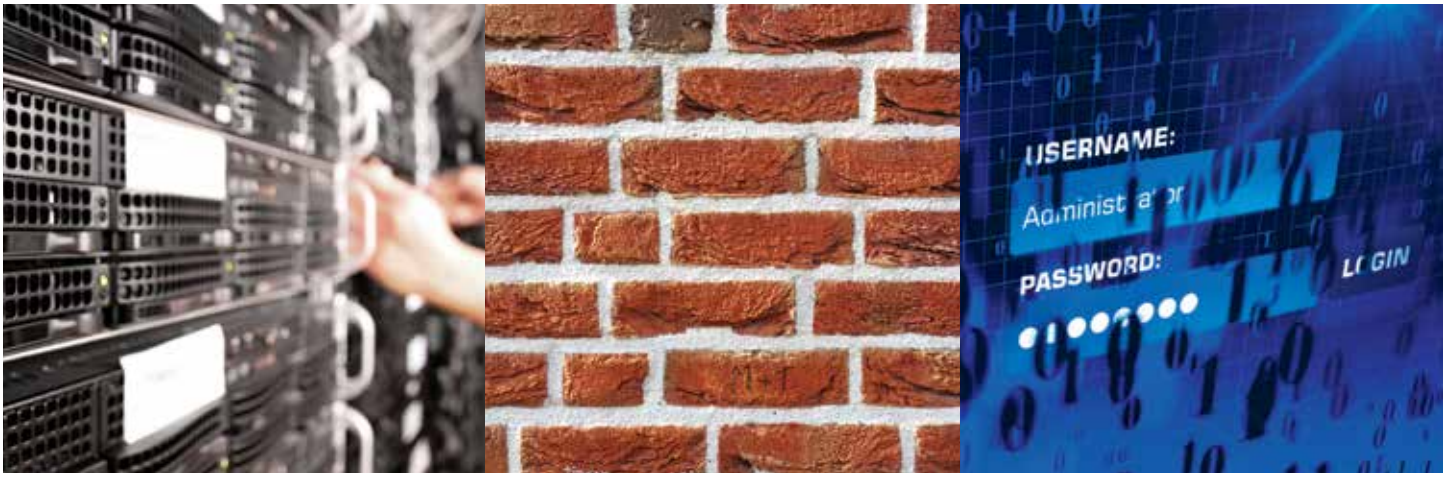
Brought to you by

RCN BUSINESS
VOICE / DATA / VIDEO

Network Security

HOW TO IDENTIFY CRACKS IN NETWORK SECURITY



Cyberattacks and security breaches are on the rise. With the rapid adoption of new technologies like the cloud, businesses large and small can no longer afford to ignore this surge. While fraudulent activity will continue to become more sophisticated, you can still prepare your company by simply educating yourself on the types of threats out there.

THREATS TO CYBER SECURITY

There are a number of ways your sensitive data can be infiltrated. Not all are as obvious as you may think.

- **Third Party Providers**

  63% of data breaches were linked to a business's third party vendor or contractor, according to Computer Weekly. Hackers will often target your vendors in order to obtain network credentials and other key information with the goal of infiltrating your business's data.

- **Social media**

  Hackers can leverage the personal information found on a person's social media profile to penetrate the individual's employer. In addition, allowing employees to access social media accounts from work computers and phones can expose vulnerabilities that hackers can use to their advantage.

- **Unclear company network security policies**

  Employees can unknowingly put a company at risk simply by visiting the wrong site and clicking various unprotected links. It's important to provide Internet guidelines, standards and enforcement policies to ensure all employees are educated on penalties for violations.

- **Bring Your Own Everything (BYOx)**

  More than ever, employees are bringing their own mobile devices, applications and cloud storage into the workplace. The amount of mobile devices is expected to reach 50 billion by 2020. This dependence on mobile devices actually leaves a company's information susceptible to threats.

STRATEGIC PLANNING

By 2018, 50% of organizations will assess the security policies of their partners to identify any risks involved with continuing the relationship.

Source: Gartner

BUSINESS DISRUPTION ATTEMPTS

The number of DDoS attacks more than doubled in Q1 2015 compared to Q1 2014.

Source: Akamai Q1 2015 State of the Internet — Security Report

BREACH SELF-DETECTION SLUMPING

The percentage of businesses able to detect a security compromise fell from 29% to 19%, year over year.

Source: 2015 Trustwave Global Security Report

RISING COSTS

Business breach costs will jump to $2.1 trillion by 2019.

Source: Juniper Research

The network security market consists of firewalls, unified threat management (UTM) systems, intrusion detection and prevention (IDP), and virtual private network (VPN) technology.

Source: IDC

AVAILABLE NETWORK SECURITY RESOURCES

There are a variety of protections that organizations can put in place to combat attacks from cyber criminals. As these threats become more sophisticated, the methods of defense must also evolve.

- A firewall is a network security system that is either hardware- or software-based. It controls incoming and outgoing network traffic based on a set of rules.
- A unified threat management (UTM) system allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.
- An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).
- An intrusion prevention system monitors network traffic. It also has the ability to take immediate action, based on a set of rules established by the network administrator.
- A virtual private network (VPN) creates an encrypted connection over a less secure network. It ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. *(http://searchenterprisewan.techtarget.com/)*

WHAT BUSINESSES CAN DO TO PREVENT CYBER ATTACKS

While threats to Internet security are growing in sophistication, there are a number of ways you can begin to protect your company.

- Update your security software frequently: New viruses are created every day in the hopes that a business will not have the most up-to-date software to combat the new threat. Manufacturers of internet security software know this and constantly make updates to prevent the latest viruses. Sign up for the automatic updates to ensure you always have the latest safeguards to protect your data.
- Protect your internet from internal or disgruntled former employees: Disgruntled employees with malicious intentions or general careless errors from current staff can often pose a more serious threat than a hacker. Implement a solid password policy such as changing passwords every 90 days, ensuring each employee uses a combination of numbers and letters, and delete the accounts or change passwords of terminated employees.
    - » Another way to limit the amount of harm an employee can do to your system would be to divide responsibilities among your employees. This way, no one individual could completely sabotage your network.
- Create a company manual dedicated to internet security: Consider putting your internet security plan to paper. A dedicated internet security manual that outlines the policies and procedures will make it harder for employees to disregard or argue.

Firewalls and antivirus software are no longer sufficient protections for businesses. It is important to constantly monitor threats and have a mindset that prepares for “when” not “if” a hack will occur. During the past several years, cyberattacks and hacks have gained a much higher profile, which should give CISOs and CIOs a good argument for better budget considerations.

While network security solutions are critical, the purchasing, deploying and ongoing management of those solutions is no simple task. When thinking about network security, there are two primary platform options to consider for your organization. A business can perform these functions in-house or outsource to a 3rd party vendor. It is often perceived that an in-house solution provides a company with more control over their systems. However, a business must consider the impact on OpEx, CapEx, and the need for a dedicated expert to create and manage an internal security solution.

Outsourcing provides many advantages including the elimination of upfront CapEx for hardware and software, and OpEx for resources to manage a solution. In addition, your company will have direct access to a dedicated and trained team of experts who are constantly focused on protecting your network from existing and new security threats. At RCN Business, we are invested in helping IT professionals manage their company's data security. We now offer a cloud-based solution that provides a robust set of benefits for IT managers.

RCN Business Managed Security maximizes protection, giving IT managers cloud-based tools to monitor their networks. The service also provides advanced protection through layered security and enables rapid deployment across new locations, along with hardware-free scalability.

Information Technology Security, also known as IT Security, is the process of implementing measures and systems designed to securely protect and safeguard information.

Source: SANS

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access.

Source: SANS

Glossary of Terms

ANTI-VIRUS

Software designed to detect and destroy computer viruses.

DDOS PROTECTION

Distribution Denial of Service (DDoS) is a type of attack during which many compromised systems target one single system, thus causing a Denial of Service attack.

FIREWALL

A network security system that is either hardware- or software-based. It controls incoming and outgoing network traffic based on a set of rules.

INTRUSION DETECTION SYSTEM (IDS)

An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

INTRUSION PREVENTION SYSTEM (IPS)

IPS monitors network traffic and has the ability to take immediate action, based on a set of rules established by the network administrator.

NETWORK DLP/RM

Data loss prevention (DLP) ensures that end-users are not sending proprietary or sensitive information outside of an organization's own network.

SSL DECRYPTION

Secure Sockets Layer (SSL) is a common protocol that manages server authentication, client authentication and encrypted communication between servers and clients.

UNIFIED THREAT MANAGEMENT (UTM)

This allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.

URL FILTERING – IP REPUTATION

Allows an organization to control access to Internet websites based on a URL list.

USER-ID BASED CONTROL

A security policy where users and user groups must enter a User-ID to access the network.

VIRTUAL PRIVATE NETWORK (VPN)

VPNs create an encrypted connection over a less secure network. It ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.