CyberSecurity: Insight & Recommendations

Cybersecurity: Technology and people have to be symbiotic.

In the past, much of the cybersecurity focus and activities by both industry and government have been reactive to the latest threat or breach. That trend appears to be changing from reacting to being more proactive. That is a good thing. The newer approach is for a more **holistic approach** of integrating technologies, processes and people.

The future of the practice will rely more on informed risk management. That requires an active strategy of detection, recognition, identification, response and remediation of threats. Advancement in area of predictive data analytics and diagnostics to index, provide network traffic analysis, and protect against further incursions is already becoming a growing area of concentration.

Technology development continues to evolve with the introduction of new **innovations** to address the cybersecurity framework that includes networks, payloads, endpoints, firewalls, anti-virus software, and encryption. This framework will provide for better resiliency and also forensic analysis capabilities. Some newer areas of cybersecurity spending will be in the areas of cloud, authentication, biometrics, mobility, automation, including self-encrypting drives.

A wide variety of technologies, protocols, SMEs working in a holistic approach will be fundamental to the success of cybersecurity. This should be inclusive in any framework and cooperative strategy as we move ahead into a new digital era.

It's easy to think because you have a small to medium-size business, cybercriminals will pass over attacking your company. The "not much to steal" mindset is common with small business owners in regard to cyber security, but it is also completely incorrect. In reality, the Federation of Small Businesses found that 71 percent of cyber-attacks happened at businesses with less than 100 employees. Even more concerning, the 2016 State of SMB Cybersecurity Report by Ponemon found that 50 percent of SMBs have had a security breach in the past year.

So why are small businesses attacked more often than larger businesses? Almost all cyber-attacks are to obtain personal data to use in credit card or identify theft. While larger enterprises typically have more data to steal, small businesses have less secure networks, making it easier to breach the network. Research suggests cybercriminals can breach thousands or more small businesses, making the size less of an issue than the network security. The lack of time, budget and expertise for proper security is a top reason for the high rate of SMB attacks. Other reasons include not having an IT security specialist, not being aware of the risk, lack of employee training, not updating security programs, outsourcing security and failure to secure endpoints.

How does your SMB avoid being a victim of a cyber-attack? Here are so clues to best practices for SMB cyber security:

Use a firewall

One of the first lines of defence in a cyber-attack is a firewall. We would recommend that all SMBs set up a firewall to provide a barrier between your data and the cybercriminals. In addition to the standard external firewall, many companies are starting to install internal firewalls to provide additional protection. It's also important that employees working from home install a firewall on their home network as well. Consider providing firewall software and support for home networks to ensure compliance.

Document your cybersecurity policies

While small businesses often operate by word of mouth and intuitional knowledge, cyber security is one area where it is essential to document your protocols. The UK Trade and Investment portal provides online training, checklists and information specifically to protect online businesses. By far the most important precautionary layer because as we know there is no such thing as 100% security so constant user vigilance is key. The best antivirus software in the world will not prevent a user from clicking on a link within a malicious email. Absolute security may not be within reach however businesses effectively tackle the risks posed by these threats by following good practice and procedures.

Information sources: Federation of Small Businesses, State of SMB Cybersecurity Report by Ponemon, Tech Pro Research cybercrime 2016
Verizon 2016 Data Breach Investigations Report Trade & Investment website

Plan for mobile devices

With 59 percent of businesses currently allowing BYOD, according to the Tech Pro Research, it is essential that companies have a documented BYOD policy that focuses on security precautions. With increasing popularity of wearables, such as smart watches and fitness trackers with wireless capability, it is essential to include these devices in a policy. We also recommend that small businesses require employees to set up automatic security updates and require that the company's password policy apply to all mobile devices accessing the network.

Educate all employees

Employees often wear many hats at SMBs, making it essential that all employees accessing the network be trained on your company's network security policies. Since the policies are evolving as cybercriminals become savvier, it's essential to have regular updates on new protocols. To hold employees accountable, have each employee sign a document stating that they have been informed of the policies and understand that actions may be taken if they do not follow security policies.

Enforce safe password practices

Yes, employees find changing passwords to be a pain. However, the Verizon 2016 Data Breach Investigations Report found that 63 percent of data breaches happened due to lost, stolen or weak passwords. According to our research, 65 percent of SMBs with password policies do not enforce it. In today's BYOD world, it's essential that all employee devices accessing the company network be password protected. Furthermore, employees be required to use passwords with upper- and lowercase letters, numbers and symbols and should require all passwords to be changed every 60 to 90 days.

Regularly back up all data

While it's important to prevent as many attacks as possible, it is still possible to be breached regardless of your precautions. We recommend backing up all your critical data including word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Be sure to also back up all data stored on the cloud. Make sure that backups are stored in a separate location in case of fire or flood. To ensure that you will have the latest backup if you ever need it, check your backup regularly to ensure that it is functioning correctly.

Install anti-malware software

It's easy to assume that your employees know to never open phishing emails. However, the Verizon 2016 Data Breach Investigations Report found that 30 percent of employees opened phishing emails, a 7 percent increase from 2015. Since phishing attacks involve installing malware on the employee's computer when the link is clicked, it's essential to have anti-malware software installed on all devices and the network. Since phishing attacks often target specific SMB employee roles, in particular Finance executive, Administration Support Personnel and Salespeople.

Make additional authentication or verification steps a requirement for any sensitive requests like wire transfers. Additionally, encourage executives to limit what they share and who they connect with on social networks. Provide admin assistants with a clear procedure for how to deal with suspicious emails and make sure you have a good spam filter in place, consider how to transfer invoices through additional methods other than email. Remind salespeople to double-check any linked text they receive in an email and discourage them from opening attachments from sources they don't know.

Use multifactor identification

Regardless of your preparation, an employee will likely make a security mistake that can compromise your data. Using the multi-factor identification settings on most major network and email products is simple to do and provides an extra layer of protection. Its recommended that employee's use their numbers as a second form, since it is unlikely a thief will have both the PIN and the password, better still consider Two Factor Authentication software (TFA).

Information sources: Federation of Small Businesses, State of SMB Cybersecurity Report by Ponemon, Tech Pro Research cybercrime 2016
Verizon 2016 Data Breach Investigations Report Trade & Investment website

Recommendations

Boundary Security

This is defined by hardware or software based solutions that protect your network from connections or to external sources, such as the Internet, Email or cloud services

Enable filtering of connections to and from the internal network. Running the IPS Software pack provides additional benefits of incident reporting and intrusion detection.

Firewalls rely heavily on professional configuration and adhering to security policies to make sure that external access in to the internal network is restricted to a minimal level. The same is also applied to traffic going from the internal network to the internet

Our Recommendation

- Juniper SRX Firewall
- IPS Software pack
- Managed configuration

Email Security

Users should be protected from SPAM, Malware and Viruses by ensuring that suspect messages are stopped at the boundary and never reach the end users inbox.

Additional security measure can also be taken against URL`s that are linked to Internet services know to contain Malware. Oncore Email Defence blocks over 60% of all emails at the edge, meaning that 60% emails are not ever transmitted. It then rejects a further 20% of messages following security scans.

Our Recommendation

- Oncore Email Defence featuring
- Anti-SPAM
- Outbreak Filters
- Grey Mail Filters
- URL re write
- Macro Detect

Encryption using Two Factor Authentication

Users connecting remotely to internal systems have to authenticate using a username and password.

Providing passwords meet complexity requirements this is quite secure. However, if a user's credentials are compromised, there is no form of defence and an attacker would have unfettered access to the internal network. Adding a second authentication level requires the user to be in possession of an encrypted token that is unique to the user. This is provided as an application on the user's phone. When a user enters their credentials they then have to authorise the request by responding to a message or typing a code which is provided by the app on the phone.

Our Recommendation

- Duo 2FA Access
- RD Gateway 2 FA
- Workstation Logon 2FA
- Device Insight policies
- Open VPN with 2FA

Server & Workstation Security

Even with all of the security at the boundary, user error, files from USB disks and browsing of legitimate websites can still pose a threat.
Anti-Virus: Anti-Virus (AV) should be deployed on workstations, servers. AV will protect from all know virus and Malware attacks. However, AV solutions rely heavily on being up to date with that latest virus definitions to be effective. Oncore AV Defender not only provides a remote deployment and managed service, it monitors for new definitions and deploys them instantly. In addition, a new Ransomware Vaccine will soon be available to provide added protection from known Ransomware.

Our Recommendation

- AV Defender (Managed)
- Ransomware Vaccine

Web Filtering

Traditionally this is deployed at the boundary, however this technology is dated and does not protect against zero hour vulnerabilities (Where threats are emerging and filters are not aware of the threat).

A Web filter allows an enterprise or individual user to block out pages from Web sites that are likely to include objectionable advertising, pornographic
content, spyware, viruses and other objectionable content. No longer is it possible to maintain databases of potentially or known suspect websites. Therefore, Web Filtering is now better deployed at the network and workstation level and has become a hybrid component.

Our Recommendation

- Cisco Cloud Umbrella
- Workstation Agent
- Network proxy

Information sources: Federation of Small Businesses, State of SMB Cybersecurity Report by Ponemon, Tech Pro Research cybercrime 2016
Verizon 2016 Data Breach Investigations Report Trade & Investment website

Data Residency, Storage and Archive

Unstructured data growth, application proliferation and increasing variation in data types continue to accelerate. This leads to increased server and storage sprawl with numerous silos of infrastructure supporting different workloads.

Our storage platform provides a massively scalable, multitenant object storage environment. It provides the security and broad support needed to enable organizations to gain the benefits of archiving, backup reduction, cloud, consolidation and more without compromising security or completely rewriting critical applications.

Our Recommendation

HCP (Hitachi Content Platform) Private, Public or Hybrid Deployment

Data Protection

- Leverage advanced replication, erasure coding and edge device integration to ensure collection and protection of content.
- Select the right level of protection with dynamic data protection levels.
- Locate the right information with ease thanks to metadata query tools, versioning and full content search.
- Move data protection or deep archive copies to spin-down disk or make tape copies if desired.

Content Preservation

- Store, retrieve and manage the lifecycle of data for long-term storage for corporate governance
- Protect and secure content for long-term preservation; content is continually checked throughout its retention period for integrity.
- Aggregate content from a variety of sources, including file servers, email and collaboration tools such as Microsoft SharePoint.
- Grow business horizontally to support multiple applications and content types and scale vertically to support continued data growth.

Content Distribution

- Connect multiple, distributed sites to a centralized content repository.
- Share content from one edge location to another via Hitachi Data Ingestor.
- Control data placement and distribute content to appropriate audiences.
- Provide bottomless, backup-free storage to branch and remote offices via Hitachi Data Ingestor.

Cloud Deployment

- Employ a single, multipurpose, unstructured data platform for archive, cloud and backup capabilities.
- Monitor and report on storage and bandwidth use for chargeback.
- Employ user tools as well as application and management interfaces for cloud and distributed environments.
- Service providers can offer bottomless, backup-free storage to customers via Hitachi Data Ingestor.

HDI (Hitachi Data Ingestor) Physical or Virtual Deployment

Hitachi Data Ingestor provides a standard connection, or on-ramp, into the core data centre without requiring application recoding and without changing the way users interact with storage today. Because HDI acts as a caching device, it provides users and applications with seemingly endless storage and a host of newly available capabilities.

Hitachi Data Ingestor presents a “standards” based file system interface that is tightly integrated with Hitachi Content Platform to provide seamless access and a wide range of advanced storage features.

HDI uses Reduce Cost and Complexity at the Edge and Simplify Cloud Deployments. Hitachi Data Ingestor use HTTP/HTTPS to securely move data over a local or wide area network and into HCP.

- Provides local and remote access to a HCP for clients over CIFS and NFS
- Delivers seemingly bottomless storage capacity, back-ended by HCP
- Migrates content to a central HCP and maintains a local link to the migrated content
- Provides file restore
- Allows content sharing between HDI systems
- Provides a management API that enables integration with the HCP management user interface (UI) and 3rdparty or home-grown management user interfaces
- Supports Active Directory and LDAP authentication for HCP clients
- Scales to 400 million files per HDI
- Employs intelligent local cache to accelerate access to HCP content over CIFS and NFS

Unstructured data growth, application proliferation and increasing variation in data types continue to accelerate. This leads to increased server and storage sprawl with numerous silos of infrastructure supporting different workloads. Our storage platform provides a massively scalable, multitenant object storage environment. It provides the security and broad support needed to enable organizations to gain the benefits of archiving, backup reduction, cloud, consolidation and more without compromising security or completely rewriting critical applications.

Most significantly, our platform eliminates the need for a siloed approach to storing unstructured content. Thanks to its massive scale, multiple storage tiers, Oncore reliability, cloud capabilities, multitenancy and configurable attributes for each tenant, the platform can support a wide range of applications on a single physical cluster. By dividing the physical cluster into multiple, uniquely configured tenants, administrators create “virtual content platforms” that can be further subdivided into tens of thousands of namespaces for additional organization of content, policies and access control.

Paul Cook Sales Team
Oncore IT
5th Floor
1 Portsoken Street
London
E1 8BT

T: 020 3818 3411
E: pcook@oncoreit.com

Conclusions

Security is a moving target. The cyber criminals get more advanced every day. In order to protect your data as much as possible, it’s essential that each and every employee make cyber security a top priority. Most importantly, that you stay on top of the latest trends for attacks and newest prevention technology. Of course, to incorporate true cybersecurity protection, it all comes down to a basic security awareness of employees, establishing security protocols, and having a trained works force. Technology and people have to be symbiotic.

Information sources: Federation of Small Businesses, State of SMB Cybersecurity Report by Ponemon, Tech Pro Research cybercrime 2016
Verizon 2016 Data Breach Investigations Report Trade & Investment website