SPONSORED CONTENT
Redmond Channel Partner

Highlights from a Webcast on Cloud Security

BEST PRACTICES FOR SECURING YOUR OFFICE 365 ENVIRONMENT

Just having a firewall is not going to provide the security you require for your Office 365 environment, argues Howard M. Cohen, Senior Resultant, HMC Write Now. He started out a recent webcast for partners by dispelling the myth that once you have Office 365 your security is no longer a worry.

Clients tend to ask: "Doesn't Microsoft secure Office 365 itself? What do we have to do?" While there is no evidence that Microsoft has lost a client's data in the cloud, and the company does have an extensive box of security tools, your client is still responsible for using those tools to protect its data. Microsoft's service level agreement for Office 365 basically says it is responsible for the infrastructure in the cloud but the client is responsible for their data. If ransomware encrypts your client's Office 365 data, that is the client's responsibility. Microsoft is not going to help you with encrypted data. The cloud infrastructure is running fine, the fact that your data is encrypted by attackers is your problem.

"No matter what," Cohen says, "your client owns responsibility for their own data and their own network. Yes, you can talk about all the provisions that Microsoft puts in, you can talk about all the different services people will provide. They don't matter. At the end of the day, the fiduciary responsibility to the stakeholders is owned by the client company."

ranjith ravindran / Shutterstock.com

So, partners need to help their customers better assure that they are fulfilling their responsibility. They need to understand that security is something they need to work on all the time. "Security is not a fit it and forget it reality." Cohen says.

What does great security look like?

"First and foremost it's multi-layered," Cohen says. The standalone firewall, the go-to security tool for many decades, it now just not enough. "Everybody thought, 'Once I have a firewall, I'm good. And all I have to do is plug in the firewall, connect it to my network, and we're good.' And nothing, believe me, nothing could be further from the truth."

Cohen suggests building a chain of security. "I like calling it a chain. I think it's a good metaphor because a chain is only as strong as its weakest link. And that's more true in security than in any place else it could possibly be. If you have a weak link, you don't have security because some bad actor will find their way to that weak link and they will penetrate and exploit that."

Besides the firewall, Cohen recommends adding the following to security:

■ **RSA Security Fob** provides two-factor authentication by adding six digits to the user's password. The six digits change every 60 seconds, so no one can determine what the number combination was when you logged on a minute ago.

■ **Role-Based Network Access Control** allows the network to recognize the device during sign-in. It inspects your device to make sure your device and you are both authentic and it knows what resources on the network you're authorized to access. It also allows you to scale access based on an individual user's role. This can be managed as Policy in Office 365 Security & Compliance Center:

- Identify, monitor & automatically protect sensitive information across Office 365
- Identify personally identifiable information such as credit card numbers in documents
- Identify and block access to any record containing health information

■ **Intrusion Prevention Systems** take many different shapes. There are many services that will scan your network and scan all the different connections that lead to your network and let you know when something's not right such as behavior at a connection is not what it's supposed to be or a user is not interacting normally. There are all manner of behaviors that intrusion prevention systems compare to its database of normal. So, the traffic that comes into the network comes to the intrusion prevention system first and if there is anything that's really strange, that's reported back to you and their entry might be held up if you set your rules to do that.

> "If you have a weak link, you don't have security because some bad actor will find their way to that weak link."
>
> —Howard M. Cohen

■ **Anti-virus software** is available that can detect and stop viruses that are often used to get a foothold into the system prior to attack.

■ **Anti-malware software** offers protection from known malware and if it is any good it will be constantly updated as new malware hits the scene.

■ **Encryption** is important for data at rest as well as data in-transit. If a hacker tries to steal your data, it will be good to have it in a form that can't be read, so things like confidential client communications aren't compromised. Encryption is the final level of protection after all others

- Microsoft encrypts data at rest in the server side and in transport
- Bitlocker protects data on the user side

All of the above help discourage hackers by making your network very unattractive.

Microsoft Security Tools You Can Use

As mentioned earlier, Microsoft has some excellent tools for securing Office 365. Its Enterprise & Mobile Security (EMS) package includes:

■ **Azure Active Directory Premium:** delivers multi-factor authentication; access control based on device health, user location; and, holistic security reports, audits, and alerts.

■ **Microsoft Advanced Threat Analytics:** helps extend the visibility, auditing, and control you have on-premises to your cloud applications.

■ **Azure Information Protection:** provides persistent data protection of files shared internally and externally, including the option to track, classify and label data.

■ **Microsoft Cloud App Security:** provides deep visibility and control of data inside cloud applications.

■ **Microsoft Intune:** makes it easier to secure and manage iOS, Android, and Windows PCs all from one console. Deep integration with Office 365 helps keep company data secure in the Office mobile apps

SherWeb Simplifies the Cloud

More than 40,000 businesses through a network of 5,000 partners in over 100 countries trust SherWeb for their cloud services. It is your one-stop shop for a full range of IT cloud solutions, such as high-performance cloud servers, cloud databases, hosted Exchange, Office 365 and collaboration tools.