WHITEPAPER

A GUIDE TO

Security and Privacy in a Hosted Exchange Environment.

Executive Summary

When it comes to deploying Microsoft Exchange, businesses are turning to the cloud in increasing numbers. That's because the cloud enables them to extend fully featured Exchange functionality without investing capital into extensive on-premises hardware and software deployments.

BUT NOT ALL CLOUDS ARE CREATED EQUAL.

As you consider hosted Exchange providers or even on-premises deployments, it's critical to look beyond functionality and pricing to elements such as onboarding, support, back-end architecture and—perhaps most importantly—security.

There are many elements of hosted Exchange security, and a good hosted Exchange provider will excel at all of them. A good provider will also constantly evaluate and update their security tools and processes. This is especially important if you plan to integrate mobile devices into your Exchange environment, because mobile technology changes at an extremely fast rate; you'll be relying on your provider to ensure the security of your environment keeps pace.

This white paper helps you make an informed decision about provider security.

WHY DOES SECURITY MATTER?

A breach in email security can have both commercial and legal ramifications. Consider the example in which your email systems are infected with a highly destructive virus. In addition to infecting your own systems, a malware-infected email could infect a customer, a partner, or even a competitor. If the malware payload is delayed, you might spread the infection even before it compromises your own system.

The commercial implications alone could be significant. They could include loss of business-critical systems and data, extensive time and resources required to restore your operations, and lost revenue and missed business opportunities.

Worse, though, is that your organization could be liable for any loss suffered by a third party as a result of the infected email, even if it was spread unintentionally. If that third party happened to be a competitor, they would be even more likely to exercise their legal right to sue for damages.

WHY HOSTED EXCHANGE IS MORE SECURE THAN AN ON-PREMISES DEPLOYMENT

A hosted Exchange provider's viability in the marketplace rests in part on its ability to offer a more secure environment than its customers could typically achieve on their own. This means that few businesses stand to lose as much in a security breach.

As such, the hosted Exchange provider will invest a great deal more in security than their customers could typically afford in an on-premises deployment.

This is especially true for physical security. At the core of every hosted Exchange provider's business are physical facilities that house their servers and network infrastructure. These datacenter facilities employ comprehensive physical security controls such as video surveillance, multi-factor employee authentication and other monitoring tools. It would generally be cost prohibitive for a small or medium-sized business to replicate this level of physical security in their on-premises email infrastructure.

CHECKLIST FOR COMPARING EXCHANGE PROVIDERS

This checklist makes it easy to compare the security offerings of potential hosted Exchange providers. (Each of these elements of security is defined in detail on the following pages.)

SECURITY ELEMENT	ON-PREMISES OR CLOUD EXCHANGE PROVIDER	OUR HOSTED EXCHANGE
Multi-tenant platform security	☐ _____ ☐ _____	✓ Redundant, enterprise-class firewalls ✓ Multiple Intrusion Prevention Systems (IPS) employed (host and network)
Physical Security	☐ _____ ☐ _____ ☐ _____	✓ Closed-circuit TV ✓ Secure access policies ✓ Security guards
Employee security	☐ _____ ☐ _____ ☐ _____	✓ Background checks ✓ Two-factor authentication and role-based access control ✓ Restricted server access
Redundant Internet service providers	☐ _____	✓ Multiple Tier-1 Internet providers
Authentication and access	☐ _____ ☐ _____	✓ Stringent caller identification procedures ✓ Admins have control over access
Dedicated security staff and monitoring	☐ _____ ☐ _____	✓ Employs dedicated, full-time certified security staff ✓ Team monitors all aspects of security

ELEMENTS OF SECURITY IN A HOSTED EXCHANGE ENVIRONMENT

To help you evaluate a potential provider's security capabilities, this section provides a list of key elements of hosted Exchange security. Any provider should be able to clearly articulate how they meet each of these standards.

MULTI-TENANT PLATFORM SECURITY

A hosting provider's datacenter is designed to service the email needs of multiple clients simultaneously. This multi-tenant environment requires vigilant security to protect against unauthorized access between accounts.

You should ask your provider how they leverage firewalls, virtual private networks (VPNs) and traffic management tools to help safeguard against malicious attacks (such as DDoS) or unwarranted access.

Intrusion protection systems (IPS) should also be in place as an added level of security beyond conventional firewalls.

PHYSICAL SECURITY

A hosted Exchange provider's datacenter should be physically protected. Physical security elements encompass surveillance cameras, perimeter security, employee access controls at each datacenter and company facility, and more.

EMPLOYEE SECURITY

A provider's vigilance for security should extend to employees themselves. A few questions you should ask: how thorough are their employee background checks? What is the primary focus and experience level of the security staff? Is security maintained by dedicated and specially trained personnel, or by the provider's general IT operations staff? What role does outsourcing play in the service provider's organization and service offerings?

REDUNDANT INTERNET SERVICE PROVIDERS

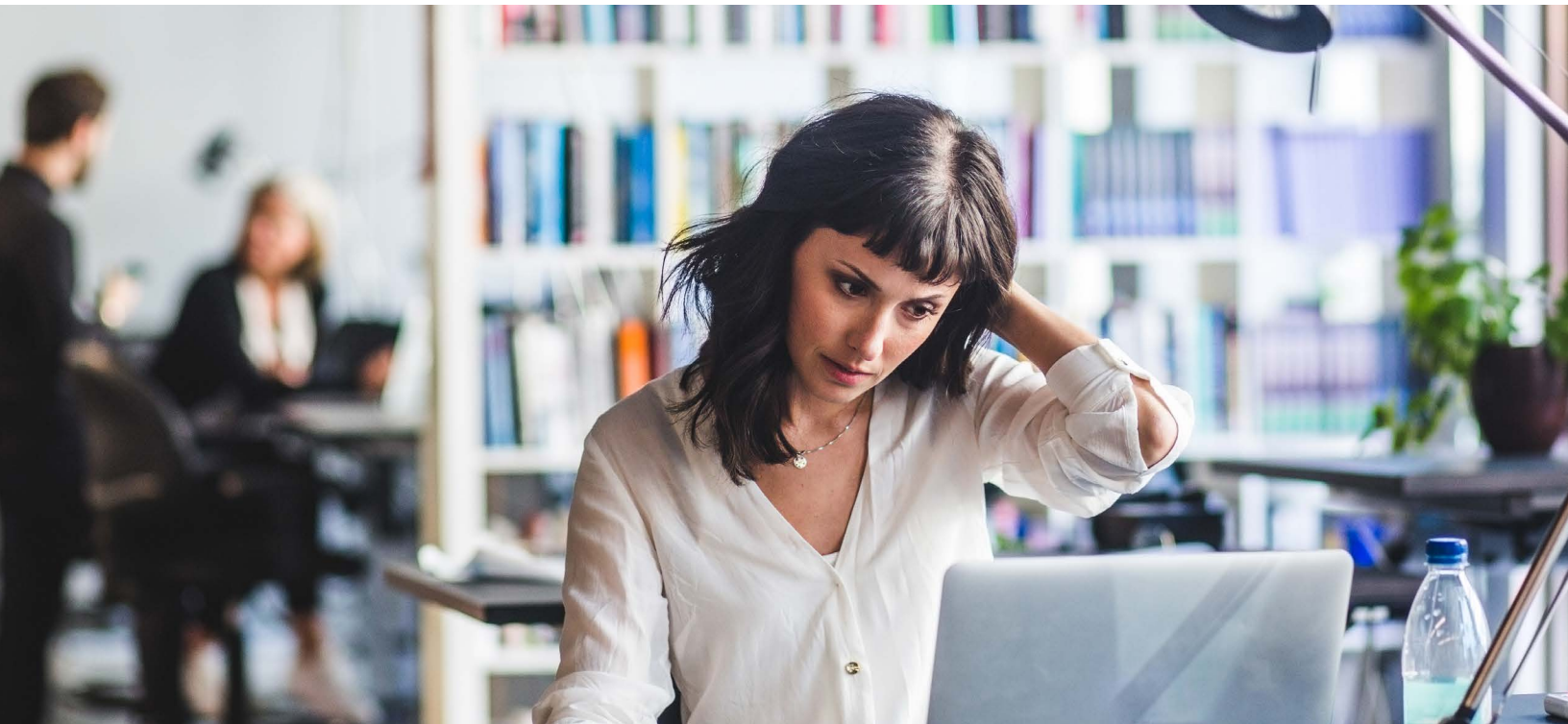
A hosted Exchange provider's dependence on Internet service providers is important. Ask your potential providers how a Distributed Denial of Service (DDoS) attack targeted against their infrastructure would impact their service, and ensure they have proper mitigation technologies in place to switch providers seamlessly if one should become unavailable.

AUTHENTICATION AND ACCESS

A provider should have clearly documented policies that govern how confidential information about your account (such as passwords and other credentials) are treated. For example: how do they verify the identity of callers who request phone support for your account?

DEDICATED SECURITY STAFF AND MONITORING

Who is in charge of the provider's security? Is there dedicated security staff, or is the staff's attention split between multiple elements of the providers' business? In either case, which elements of security does the provider's staff monitor—and which ones, by implication, are left for you to monitor?



HOW WE ENSURE HOSTED EXCHANGE SECURITY

Now that you understand the key security capabilities to seek in a hosted Exchange provider, let's take a closer look at how we address addresses these requirements.

MULTI-TENANT PLATFORM SECURITY

We use multiple redundant, enterprise-class firewall systems to help prevent unwarranted intrusions and to help ensure only authorized users access your Exchange environment. This purpose-built security system integrates firewall, VPN and traffic management.

We also run multiple intrusion prevention systems (IPS) (both host and network) to help detect and deter malicious network traffic and computer usage that often cannot be caught by a conventional firewall. The system monitors for unusual traffic patterns and alerts system administrators of any suspicious behavior. IPS can also help prevent network attacks against vulnerable services; data driven attacks on applications; host-based attacks such as privilege escalation; unauthorized logins and access to sensitive files; and malware (e.g. viruses, Trojan horses, and worms).

PHYSICAL SECURITY

Each of our datacenters adheres to strict standards in physical security. Each datacenter is closely monitored and guarded 24/7/365 with sophisticated pan/tilt closed-circuit TVs. Secure access is strictly enforced using the latest technology, including electronic man-trap devices between lobby and datacenter, motion sensors and controlled ID key-cards. Security guards are stationed at the entrance to each site.

EMPLOYEE SECURITY

Every employee, regardless of role, undergoes a rigorous background check. Employee access to passwords, encryption keys and electronic credentials is strictly controlled using two-factor authentication and role-based access control. Access to servers is restricted to a limited number of authorized engineers and monitored regularly

REDUNDANT INTERNET SERVICE PROVIDERS

Each of our datacenters is serviced by multiple Tier-1 Internet providers to mitigate the potential impact of a Denial of Service (DoS) attack on any single provider.

AUTHENTICATION AND ACCESS

We have established a number of stringent policies and procedures to authenticate a caller's identify during support and service calls. These policies and procedures help protect confidential information belonging to your account and to your users by helping to ensure that only authorized members of your team are given access to our services. In addition, our online control panel enables administrators to fully control access to services and administrative functions.

DEDICATED SECURITY STAFF AND MONITORING

We employ dedicated, full-time security staff who are certified in all disciplines of information security. This team is involved with all aspects of security, including log and event monitoring, incident response, managing intrusion detection systems (both host and network), perimeter defense, service and architecture testing, and source code reviews.

CONCLUSION

Many hosted Exchange providers will advertise the latest software, the fastest servers, and the most advanced datacenters. But in order for you to trust this critical business tool to their cloud, their services must be backed up by the highest levels of security.

As you search for a hosted Exchange provider that best matches your organization's needs, be sure to give security the priority it deserves.

QUESTIONS? CONTACT US TODAY!

Leap of Faith Security
3024681831
sales@leapoffaithsecurity.com
www.leapoffaithsecurity.com