IN THIS CHAPTER

- Understanding cloud computing and its value in the current threat landscape
- Getting to know the cloud deployment and service models
- Determining the right Office 365 plan for your organization

Chapter 1

Understanding Cloud Computing and the Current Threat Landscape

The way we work today is vastly different from the way we worked in the past. Gone are the days when we worked from 9 a.m. to 5 p.m. in one location using one desktop computer and software that didn't connect to the Internet. Today we get our work done using a desktop, a laptop, a smartphone, or a tablet while on the bus, at the doctor's office, during a run, at a coffee shop, and even when we're on vacation.

Welcome to the new world of work. It is the way most organizations are working, and it is the way the modern and younger workers expect to work.

As more companies embrace the opportunities presented by cloud and mobile computing, they also take on new risks. One of the most significant challenges in today's computing environment is ensuring security, privacy, and compliance. In fact, there is a consensus in the business world that there are only two types of

organizations: those that know they've been hacked, and those that don't know they've been hacked. By the end of 2017, more than 28,800 data breaches had occurred globally with over 19 billion — again, that's *billion* — records exposed stemming from over 20,000 types of vulnerabilities.

The security issues we know today are not isolated to Fortune 500 companies. The reality is that small and medium-sized businesses (SMBs) are just as vulnerable to attacks. In fact, SMBs face more serious risks for a variety of reasons, including the scarcity of security talent in the industry; their inability to identify, assess, and mitigate security risks; the lack of familiarity with security best practices and the overall threat landscape; and confusion from the multitude of security solutions from which to choose.

One might conclude that the best defense against cyberattacks is to have a computing environment that's not in the cloud (rather *on-premises,* as technologists call it), and is protected by firewalls using the best encryption technology and running the latest anti-virus software. The problem with this approach is that all it takes to start a breach is one simple human error, such as clicking on a link or opening an attachment in an email. The reality is that as software and platforms are getting better at combatting cyberthreats, attackers are shifting their focus to the human element to hack the users through social engineering.

But what is *social engineering?* Consider the following real-life example:

Cloud611, a Microsoft Cloud Solutions Provider, resells Office 365 licenses to SMBs. Recently, a customer forwarded an email to Cloud611 asking why the company was warning him that his account could be deleted or closed. The exact language of the email read:

> *Your account will be disconnected from sending or receiving mails from other users because you failed to resolve errors on your mail.*
>
> *Confirm your activities* here*.*
>
> *Regards,*
>
> *The Mail Team*

Under the guise of being a solutions provider, the attacker tried to use a scareware tactic to trick the customer into clicking on the word "here," which is hyperlinked to a site that then downloads and installs malware on his computer. Fortunately, the customer did not completely fall for it, and the attacker failed — this time.

Social engineering comes in many forms: phishing, spear phishing, scareware, and more. These tactics all attempt to psychologically manipulate a user into divulging information or influence an individual to perform a specific action. The end game is usually to gain access to the computing environment to do harm.

The good news in this story is that the customer did not have to invest thousands of dollars to implement an end-to-end security solution nor hire an expensive security expert to protect his small business. For a mere $2 per user per month, the customer added Advanced Threat Protection (ATP) to his Office 365 Business Premium license to secure his mailboxes, files, online storage, and even his Office applications against advanced threats.

This chapter is for those of you who have a keen interest in understanding the basic principles of cloud computing with the intent of utilizing the benefits of the cloud to run your business in a way that increases employee productivity while keeping your environment secure. It covers the various services offered within Office 365, including what they cost and the latest security and privacy features built into the services. With the knowledge you gain from this chapter, you will be better prepared run a more secure, productive organization.

Understanding Cloud Computing

The "cloud" is a metaphor for the "Internet." In simplistic terms, *cloud computing* means that your applications or software, data, and computing needs are accessed, stored, and occur over the Internet "in the cloud."

If you've had a Facebook account, played online games, shared files with Dropbox, or shared a photo of your new haircut on Instagram, you've been computing in the cloud. You're using the services of an entity to store your data, which you can then access and transfer over the Internet. Imagine what life would be like if you wanted to share photos of your lunch with all of your 500 friends and cloud computing didn't exist.

For businesses and other organizations, cloud computing is about outsourcing typical information technology (IT) department tasks to a cloud service provider who has the experience, capability, and scalability to meet business demands at a cost that makes sense.

For example, let's look at a small business such as a boutique accounting firm that services over 200 businesses locally. Email is a critical communication platform for the firm. To be productive, the firm decided to hire an independent IT consultant to install an email server in the office. The deal was that the IT consultant would train a couple of people from the firm to do basic server administration. Beyond the basics, the consultant would be available to remotely access the server to troubleshoot or show up in person if something breaks.

Like most horror stories we've heard from people who try to manage their own servers without a highly trained IT staff, the situation turned out to be a nightmare for this firm. The email server went down during tax season when the IT consultant wasn't immediately available. In an industry where highly sensitive data is exchanged and customer trust is paramount, you can imagine the stress the company owner experienced dealing with email that contained sensitive attachments ending up in a black hole, irate customers who didn't get a response to their time-sensitive requests, and lost opportunities beyond quantifying.

Cloud computing for members of this firm meant migrating their email to Office 365. So instead of running their own email server, fixing it, patching it, hounding their IT consultant, and dreading another doomsday, they simply paid a monthly subscription to Microsoft, which is the entity responsible for ensuring the services are always up and running. They also know that email will not be lost, because they don't rely on one piece of equipment getting dusty in a corner of their office break room. Instead, they're taking advantage of Microsoft's huge and sophisticated data centers to replicate and backup data on a regular basis.

The basic premise of cloud computing is that organizations of any size can take advantage of the reduced cost of using computing, networking, and storage resources delivered via the Internet while at the same time minimizing the burden of managing those complicated resources.

Breaking down the cloud deployment models

Not all organizations are created equal. For example, a financial organization has different requirements than a nonprofit organization or a government organization. To address these varied needs, cloud service providers offer different deployment options.

Public cloud

The type of deployment model the boutique accounting firm used in the previous section is referred to as the *public cloud,* where the cloud computing service is owned by a provider (Microsoft) and offers the highest level of efficiency in a shared but secure environment. The firm did not own or maintain any hardware. It accessed and used the email and other services from the public cloud on a subscription model. In cloud computing-speak, this firm is referred to as a *tenant* in a public cloud. There are multiple tenants in a public cloud. Each tenant is isolated from the other with security boundaries so there is no data leakage. As illustrated in Figure 1-1, Enterprises A, B, and C can access the same application services in a public cloud, but their data is isolated from each other.

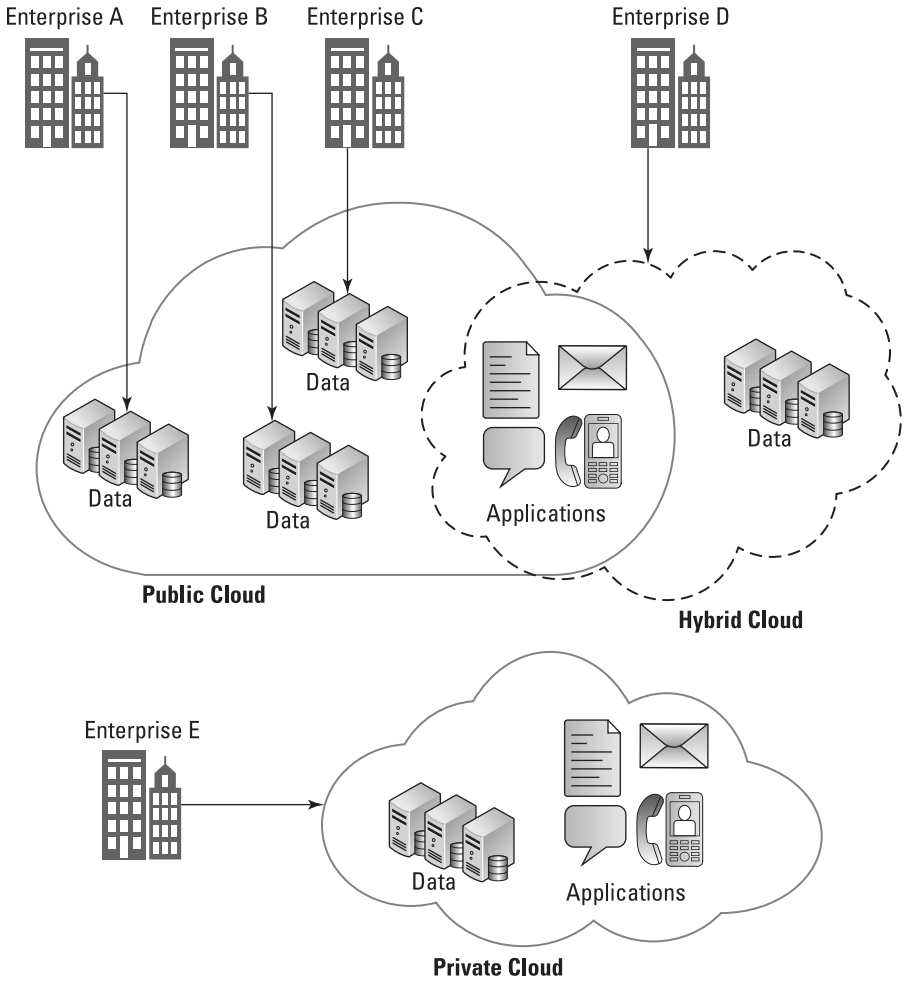

FIGURE 1-1: Cloud computing deployment models.

Using a public cloud is like using electricity. You only pay for what you use. And just like electricity, you don't need to maintain the power plants — the provider does that. You only maintain the devices using the electricity. In this example, you don't need to maintain and patch the servers running your cloud services, but you do need to maintain the computers and laptops accessing or using the cloud services.

Private cloud

A *private cloud* typically is dedicated to one organization on its own highly secure, private network located at a company's on-site data center or at a colocation facility or *colo*. A colo is a data center facility that rents space for servers to other companies.

Unlike the public cloud, a private cloud doesn't share computer, networking, and storage resources with other tenants. This allows for a higher degree of flexibility in customizing the cloud environment, as any configuration done in a private cloud only applies to that environment. Industries with privacy concerns such as financial institutions and healthcare organizations typically opt for a private cloud. The same is true for government organizations, which have more stringent security and privacy requirements.

Hybrid cloud

A *hybrid cloud* is simply a combination of the public and private clouds. For example, an organization may run its email applications in a public cloud, but store customer information in a database in a private cloud to meet business and regulatory requirements. This scenario can be seen as the best of both worlds because an organization can maintain control of the resources it is running on the private cloud, while at the same time take advantage of the scalability of the public cloud to quickly provision additional resources to meet spikes in demand. This is called "cloud bursting."

Regardless of the deployment model used, cloud computing has afforded organizations of any size the flexibility of being able to scale resources up or down based on its needs at a faster pace and lower cost than before. In fact, cloud computing is the greatest equalizer for businesses as it breaks down the barriers for small and even one-man-show businesses from competing in the global market. For a small monthly fee, any business can use the same productivity tools and built-in security features that large enterprises use.

Knowing the common cloud service models

Contrary to general belief, cloud computing isn't a new concept. The idea of an "intergalactic computer network" was first introduced in the 1960s by J. C. R. Licklider, one of the most influential men in the history of computer science. Other people attribute the emergence of cloud computing to John McCarthy, another computer scientist who in the 1960s proposed that computing be delivered as a public utility similar to service bureaus that provided services to businesses for a fee.

Back then, massive computing was conducted with supercomputers and mainframes occupying whole buildings. Thousands of central processing units (CPUs) were connected to divide the computing tasks of supercomputers in order to get results faster. The high cost of creating and maintaining these supercomputers precipitated the discovery of more economical computing means, which brings us to where we are today.

With cloud computing today, not only can businesses use the services of specialized providers for massive computing, they also benefit from the lower cost of these services stemming from the efficiencies of shared infrastructure. Generally, there are three types of cloud computing service models (see Figure 1-2):

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

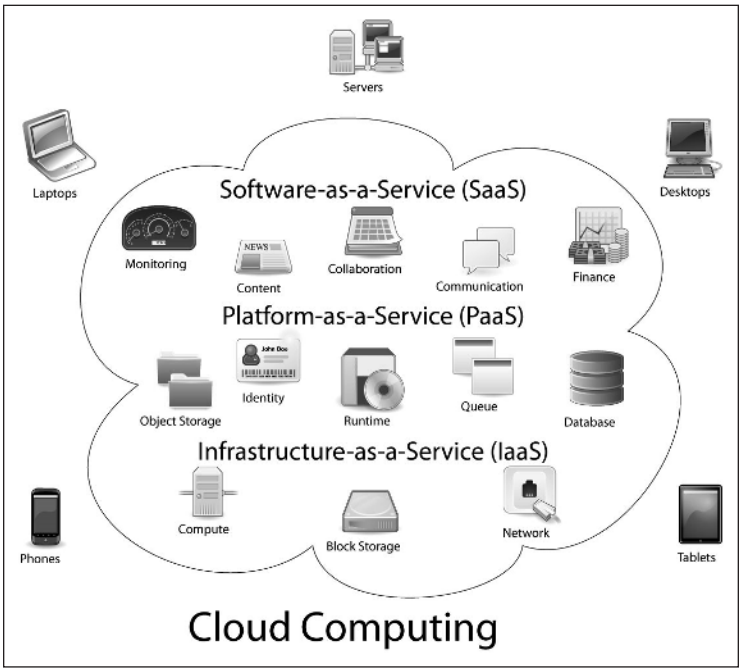

FIGURE 1-2: Cloud computing service models.

Illustration created by Sam Johnston using OmniGroup's OmniGraffle and Inkscape. Computer.svg courtesy Sasa Stefanovic.

Software as a service (SaaS)

A software as a service (SaaS) service model is where a software application is paid for on a subscription basis and installed from the cloud provider's data center. Office 365 is an example of a SaaS model where all your collaboration and productivity applications are bundled together as part of your subscription. You don't have to run your own email servers, for example, nor do you need to maintain and update the servers. For desktop applications like Office 365 Pro Plus, you can install the software from a web-based portal instead of buying the packaged

software from a store. After you've installed the software, updates and bug fixes automatically are installed in the background.

Platform as a service (PaaS)

In a platform as a service (PaaS) service model, developers can create online applications ("apps" for short) in platforms provided by the PaaS provider. The developers develop their own code for the apps, store it in the PaaS provider's data center, and then publish the apps. They don't have to worry about planning for capacity, security, or managing the hardware to run the apps — the PaaS provider does that. A PaaS model also cuts the time it takes to develop apps because of the availability of pre-coded application components such as workflows, security features, search, and so on. To some extent, PaaS is similar to creating a macro in Microsoft Excel where you use the built-in components of the software to run a code that automate tasks.

Infrastructure as a service (IaaS)

In an infrastructure as a service (IaaS) service model, organizations have access to computing power, network connectivity, and storage capacity, using a cloud provider's hardware. This model enables organizations to have control over the infrastructure and run applications in the cloud at a reduced cost and at a faster pace. The organization, however, is responsible for managing and updating the operating system running the applications. While capacity planning, security, and hardware management is the responsibility of the IaaS provider (similar to PaaS), it is the organization's job to monitor the performance of its apps and/or add more resources to meet the demand. Amazon Web Services (AWS) offer several IaaS cloud-hosting products that can be purchased by the hour. Rackspace is another player in the IaaS market offering managed and cloud hosting services. Microsoft Azure started out with a PaaS offering, but has since extended its services to include robust IaaS capabilities.

Determining the Right Office 365 Plan for Your Organization

Office 365 is a SaaS solution running in the public cloud offered on a subscription basis by Microsoft. Each subscription is comprised of one or more licenses depending on the organization's needs. Subscriptions can be purchased directly from Microsoft or through a Microsoft Cloud Solutions Provider (CSP). When you purchase your subscription directly from Microsoft, your support comes from Microsoft. If you purchase your subscription from a CSP, support for the services is provided by the CSP.

TIP

It is important to note that Office 365 comes in two versions: Home and Business. As the name implies, the Home version is intended for home use and does not include the productivity solutions such as Exchange Online or SharePoint Online, which are typically used by businesses for productivity and collaboration. This book is focused on the Business version of Office 365, which includes various plans to meet the needs of small business, enterprise, government, education, and nonprofit organizations.

Choosing between Small Business and Enterprise plans

Office 365 comes with four key technologies (or "workloads" as your IT team might call it):

- **Exchange Online:** A messaging application that powers business-class email.
- **SharePoint Online:** A web-based collaborative platform that is typically used for online storage, document collaboration, intranets, and more.
- **Teams:** Formerly called Skype for Business, the technology behind web and audio conferencing, chats, screen sharing, voice communication, and more.
- **Office Applications:** Productivity tools including Outlook, Word, PowerPoint, Excel, Access, and more that are available in both desktop and online versions.

In additional to the four key technologies listed here, the Office 365 suite also comes with a host of other features, some of which may only be available in the Small Business plan, such as Microsoft Bookings, and others that are available in all plans, such as Planner, StaffHub, Forms, PowerApps, and more. As a SaaS solution, Office 365 will continue to evolve, so don't be surprised to find new features in your subscription that may not be covered in this book.

TIP

You can view what services and features are currently available across the various Office 365 plans from the following link:

`https://technet.microsoft.com/en-us/library/office-365-platform-service-description.aspx`

While it's true that all organizations should have access to productivity and security tools, not all organizations need the same bells and whistles to run their business or pay the same price for the services. It doesn't make sense for a small business, for example, to pay the same fees as a large enterprise that has more advanced needs such as eDiscovery for legal purposes.

To address this need, Microsoft designed a variety of plans and subscriptions from which organizations can choose. There are, however, so many plans, subscriptions, and license combinations that sometimes it can be difficult to know which one is right for your organization. To help narrow down your options, refer to the decision tree shown in Figure 1-3 to quickly determine what's best for you by answering three questions.

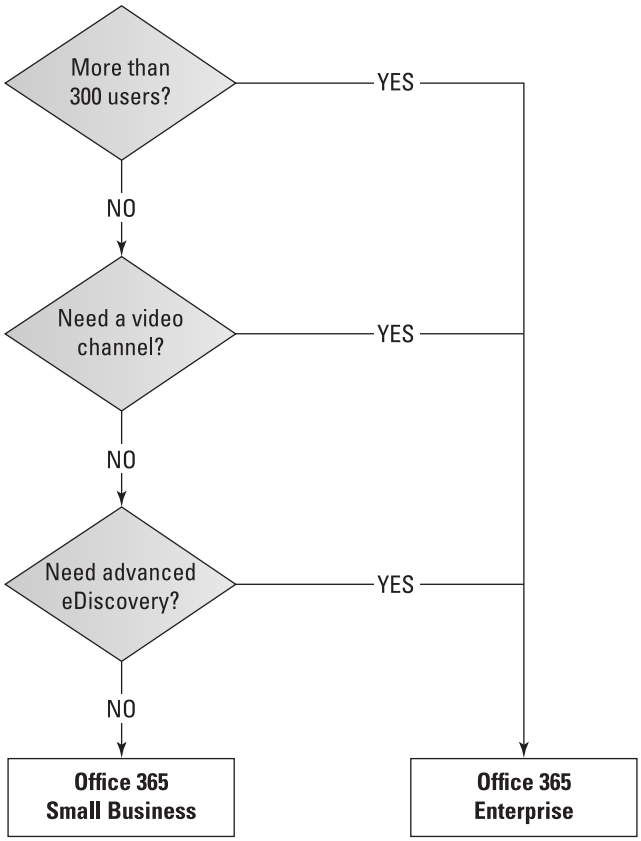

FIGURE 1-3: Small Business or Enterprise plan decision tree.

Office 365 Small Business

The Small Business plans are designed to meet the typical needs of small businesses with 300 or fewer users. There are three key offerings in the Small Business plans:

- **Office 365 Business:** $8.25 per user per month; ideal for users who only need the Office desktop applications and access to online storage.

- **Office 365 Business Essentials:** $5 per user per month; ideal for users who need business-class email and collaboration tools but do not need the Office desktop applications.
- **Office 365 Business Premium:** $12.50 per user per month; ideal for users who need business-class email and collaboration tools and the Office desktop applications.

For small and mid-sized nonprofits, Microsoft offers two plans that correspond to the Business Essentials and Business Premium plans but at zero cost and $3 per user per month, respectively.

Office 365 Enterprise

There are four key offerings in the Office 365 Enterprise plans ranging from $8 per user per month to $35 per user per month:

- **Office 365 ProPlus:** $12 per user per month; ideal for users who only need the Office desktop applications and access to online storage.
- **Office 365 E1:** $8 per user per month; ideal for users who need business-class email and collaboration tools but do not need the Office desktop applications.
- **Office 365 E3:** $20 per user per month; ideal for users who need all the features in Office ProPlus and E1 plus security and compliance tools such as legal hold, retention policies, data loss prevention policies, and more.
- **Office 365 E5:** $35 per user per month; ideal for users who need all the features in the Office 365 E3 plus advanced security functionalities, analytics, and voice capabilities such as the ability to make and receive phone calls or allow meeting participants to dial-in to a meeting for audio conferencing. Please note that there is an additional fee of $24 per user per month to make domestic and international calls. For domestic calls only, the fee is $12 per user per month.

TIP

You can mix and match a variety of enterprise subscription plans based on the needs of your users, and there is no limit to the number of users on the enterprise plans.

The education, government, and nonprofit sectors have corresponding Enterprise plans. The education plans are called A1, A3, and A5; government plans are called G1, G3, and G5; and nonprofits are called Nonprofit E1, Nonprofit E3, and Nonprofit E5. Take note that prices are different for these sectors, so check with your CSP or at `https://office365.com`.

Taking care of the firstline workforce

If you run a business with deskless workers, shift workers, retail store employees, truck drivers, or similar employees, you probably don't need all the features from any of Enterprise plans. Most of these workers share a PC or work out of a kiosk and have minimal collaboration requirements and limited communication needs. It doesn't make sense for these workers to pay the full price for plans that have more features than they need or exclude them from the benefits of using Office 365.

To solve this challenge, Microsoft designed an offering called Office 365 F1 that is targeted for the "firstline workforce." For $4 per user per month, the F1 plan gives this workforce most of the productivity and collaboration tools focused on these key areas:

- Schedule and task management
- Communications and community
- Training and onboarding
- Identity and access management

Getting to Know the Security Features in Office 365

When Office 365 was first launched in 2011, most of the pushback from organizations about using the service was around security. People were worried that having their data in the cloud would make them more vulnerable because they don't have full control of the environment. Today, it's exactly the opposite. More organizations are moving to the cloud because of security reasons. They are realizing they don't have the budget, manpower, and expertise to outsmart the attackers who are getting more sophisticated every day, so they rely on companies like Microsoft — with its highly trained engineers and robust infrastructure — to combat cyberattacks.

Especially for small and mid-size companies, it doesn't make sense to invest thousands of dollars to implement an end-to-end security infrastructure, hire top talent, and stay on top of the cybersecurity trends when they can pay for the service at a fraction of the cost.

Every month, Microsoft scans 400 billion emails for malware and phishing attacks from Office 365 and Outlook. 450 billion authentications are processed by Microsoft every month from its 200-plus cloud consumer and commercial services globally. In addition, Microsoft has scanned more than 18 billion Bing web pages

and collected data from 1 billion Windows devices. These insights provide Microsoft with visibility into the current threat landscape like no other company can. On top of that, Microsoft is investing $1 billion in cloud security every year. So, if any company is well-positioned to address security challenges in today's computing environment, it would be Microsoft.

Stepping through the anatomy of a modern attack

In Hollywood, con men or women typically are portrayed as well-dressed, suave, and attractive. Whether it's *Ocean's 11* or its all-female version, *Ocean's 8*, the con artists are smart, methodical, and manipulative.

Today's hackers are similar to con artists portrayed in movies with the advantage of not needing to be well-dressed, suave, or attractive. The con does not even require the con artist to be physically close to the target. With social engineering, hackers are able to carry out a con from hundreds of miles away in the comforts of their dorm room — or parent's basement.

The 2015 Data Breach Investigations Report published by Verizon illustrated that attacks can happen very fast. Here's what the statistics tell us in simple terms:

- If a hacker sends a phishing email to 100 people in an organization,
- 23 people will open the email,
- 11 people will open the attachment, and
- the median time it took users to make the first click is 1 minute and 22 seconds.

If you think you are immune from social engineering, think again. Hackers have gotten so good at this to the extent that your best line of defense is to acknowledge that at some point, you're going to get hacked and therefore, you need to have a plan in place to recover from it. To plan your defense, it's helpful to understand the mindset of a hacker and the anatomy of an attack.

The recon

Just like the Hollywood con movies, a cyberattack typically involves planning and preparation. Hackers have figured out that it's better to focus on human weaknesses than fight security-hardened software or platforms. A starting point for them is usually doing a reconnaissance or *recon* to figure out who the targets are. Believe it or not, there are actually free tools on the Internet to help with this effort, such as Maltego Teeth or a practice called Google Dorking, which is a

technique of applying advanced Google searches to discover confidential company information.

From reading the news, we are seeing a rising trend of attack on not just small business but also on local governments. For the most part, the hackers are not necessarily targeting a particular person or public organization but rather, their recon is focused on who is vulnerable. The recent attack on the town of Rockport, Maine in April 2018 that forced the town of 3,400 to suspend operations was due to an attacker inserting malicious software in its network through a vulnerable backup server.

The initial breach

Once the targets are identified, the breach is initiated via phishing scams or other social-engineering methods. Modern hackers have realized that phishing emails are so common that people now know how to deal with them, so they've started putting malicious macros and code within Word or Excel documents or within a PDF file. An example of this may be a hacker posing as a vendor asking an employee to open an "invoice" posted in an organization's file share or document library. As soon as the employee opens the file, the breach is initiated.

The elevation of privileges

Once the attackers gain access to the target's environment, they then use tools to get a dump of all the users in the organization. From there, they then figure out who the administrators are. Admins are the best because they have a lot of power in the IT environment. Once the attackers have the credentials of the admins, they can pretty much do anything they want to do in the environment.

The entrenchment

The entrenchment is the scary part. This is the stage when the attackers typically get really sophisticated. While the duration has gotten shorter as to how long attackers are stealthily and merrily beep-bopping along the breached environment, studies have shown that it still takes an average of 99 days between the initial breach and the detection of the attack. That's three months the attackers have to start impersonating users, delegating permissions, injecting mail-forwarding rules, and more.

The exfiltration

The culmination of an attack is the extraction of the data to be used for further attacks, ransom, sale on the dark web, or to simply embarrass a person or an organization. From leaked celebrity nude photos to ransomware to stolen medical records, there is no shortage of ways hackers can create grief for their targets or make tons of money with the payload from their attacks.

Overview of the built-in security in Office 365

Security in a cloud-computing environment is a partnership between the tenant organization and the cloud service provider. Both parties have responsibilities that, if done right, will enhance the security posture of an organization.

In Office 365, Microsoft, as the cloud service provider, takes care of the physical security of its data centers where all of its customers' data is stored. It has 24-hour monitoring and biometric scanning technologies implemented to secure the access to its data centers. Faulty drives and hardware are not taken out of the data centers — they are demagnetized and destroyed in huge shredding machines.

Microsoft has policies in place to limit human access to customer data. It has dedicated threat-management teams whose sole job is to proactively anticipate, prevent, and mitigate malicious access. The networks are constantly scanned for vulnerabilities and intrusion.


TECHNICAL STUFF

Data sitting on servers at the data centers is encrypted by default. This is called *encryption at rest.* When data moves from one data center to another, for example when sending and receiving email, that data is also encrypted. That is called *encryption in transit.* What encryption does is prevent someone from reading the content of your email even if that person manages to intercept the email during transit.

If your Office 365 plan comes with Exchange Online, you automatically have Exchange Online Protection or EOP. This service is what filters your incoming or outgoing email from spam, viruses, malware, or email policy violations, all to keep your environment safe.

On the customer side, there are tasks a tenant admin can do and actions end users can perform to enhance security. An admin can implement multi-factor authentication (MFA), which requires a user to prove his or her identity using a second factor such as a phone. If you've ever been asked by your mobile banking app to enter a code sent as a text message after you've entered your username and password, you're interacting with MFA.

Office 365 admins can implement policies to prevent users from accidently leaking confidential data. For example, an admin can create a policy that will prevent a user from sending an email if the email contains a string of characters that look like a credit card number or social security number.

Mobile device management (MDM) is another way for admins to increase security in the organization. For example, if a user loses his phone or laptop, an admin can

remotely wipe the data from those devices so that even if someone finds the device and manages to log in, all the corporate data will no longer be present on the device.

Office 365 also offers advanced security functionalities such as the ability to send encrypted email to recipients outside of Office 365 (for example, to people with Gmail accounts). This feature, called Office 365 Message Encryption, is available in the E3 license. With an E5 license, Exchange Online Advanced Threat Protection is built-in, so if a user inadvertently clicks on a bad link, it won't cause damage because links are first "detonated" in a virtual machine in the Microsoft cloud. In essence, if a link is good, the user will be taken to the site; if the link is bad, the user will be blocked and a notification will display warning the user of the suspicious link.

Managing security and privacy in a single dashboard

The Security and Compliance Center in Office 365 (see Figure 1-4) is your one-stop-shop to manage policies, reports, investigations, security posture, and even compliance with GDPR, a European Union (EU) regulation that took effect on May 25, 2018. GDPR stands for "General Data Protection Regulation" and is designed to serve and protect the personal data of all EU citizens.

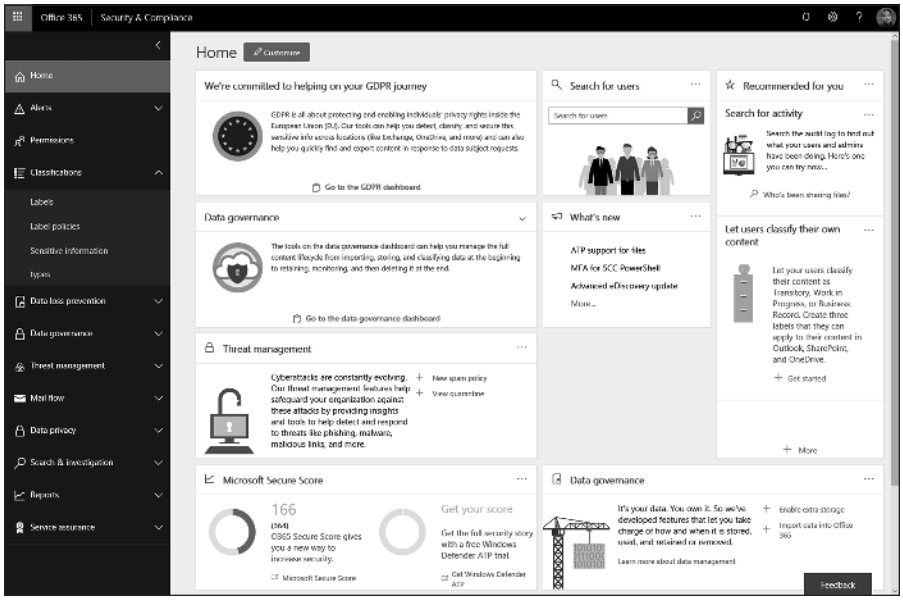

FIGURE 1-4: The Office 365 Security and Compliance Center dashboard.

The dashboard also provides a link to Microsoft Secure Score, a security analytics tool designed to help you understand what your current risk profile is and how you can improve your security posture (see Figure 1-5).

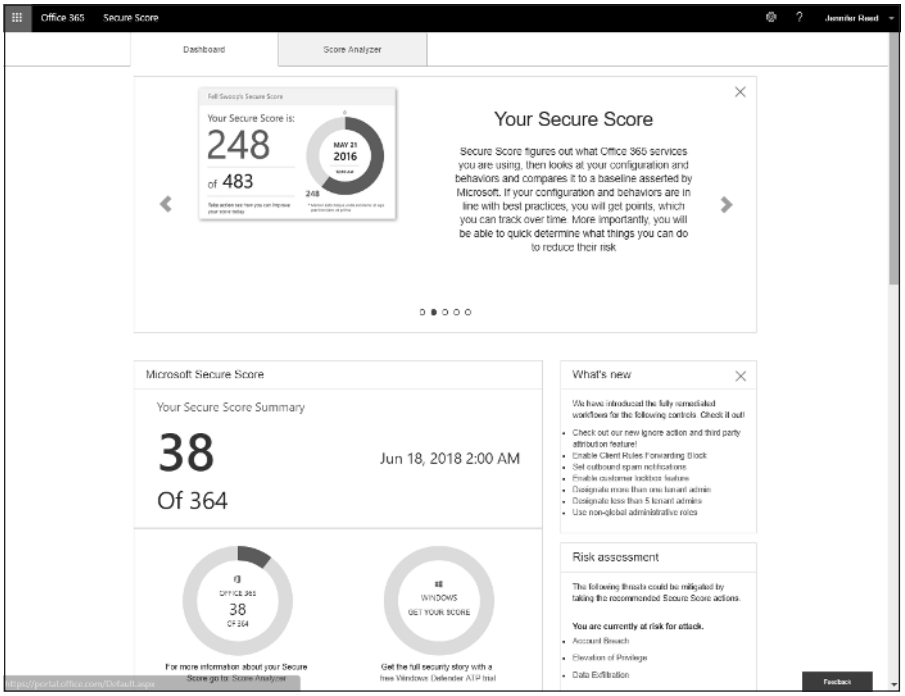

FIGURE 1-5: The Microsoft Secure Score dashboard.

Updating the anti-spam settings

An Office 365 Global Admin can create custom policies or update existing policies in the Security and Compliance Center. If you're an admin and would like to mark a certain user or domain as spam and apply that policy to your entire organization in Office 365, follow these steps:

1. **Navigate to `portal.office365.com`.**
2. **Click the Admin icon.**
3. **From the left pane, expand the Admin Centers group by clicking the arrow pointing down next to the label.**

4. **Click Security & Compliance from the list of options.**

   You are taken to the Security and Compliance Center dashboard.

TIP

   You can also go directly to the dashboard by following this link: `https://protection.office.com`. However, it is recommended that you log in to the Office 365 portal first because this link may change as Microsoft works to consolidate its numerous portals and online assets.

5. **Expand Threat Management in the left pane and click Policy (see Figure 1-6).**
6. **Click the Anti-spam card.**
7. **Scroll down and expand the Block Lists group.**
8. **Click the edit icon next to Block Sender and enter the email address of the sender you want to block.**

   This will prevent this sender from sending email to your entire organization.

9. **Click Save.**
10. **Click the edit icon next to Block domain and enter the domain you want to block.**
11. **Click Save.**

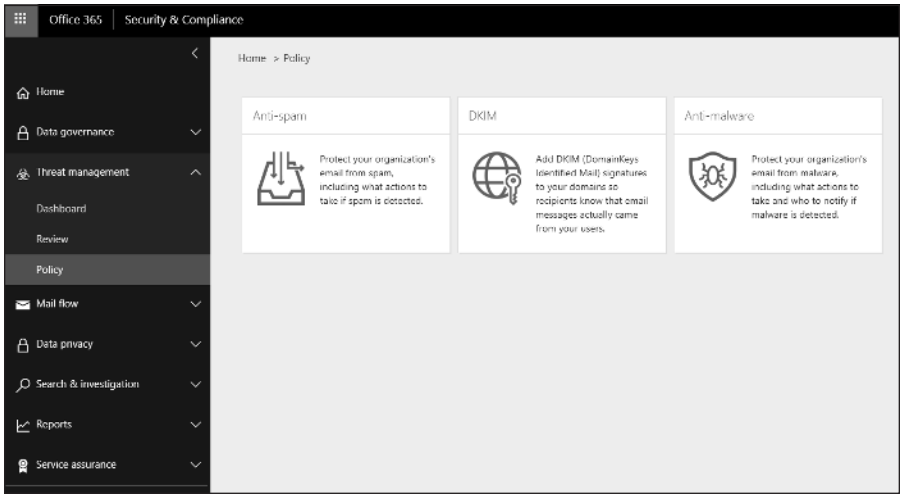

FIGURE 1-6: Updating the anti-spam policy settings.