Microsoft Digital Defense Report 2020

SUMMARY

umbrella managed systems

“Personally owned, unmanaged devices that access organizational resources are a security risk associated with remote workforces.”

- Microsoft Digital Defense Report 2020

At the end of every year, Microsoft releases a report summarizing the cybersecurity insights gained over the preceding twelve months.

The first was in 2005 and for 2021 their Digital Defense Report 2020 offers a comprehensive picture of the current state of cybersecurity. In this resource, we will distill the report’s 88 pages down to the key takeaways for the small and medium-sized organization.

Download the full report from Microsoft's website.

Report Highlights

The unexpected health crisis of 2020 forced most of the world to adapt to new, virtual ways of working.

Countless web applications and online collaboration platforms became common, and hundreds of millions of workers worldwide left their managed networks and began logging in and sharing data from less-secure public or private home connections. This risk factor was reflected in the report's finding that more than 50% of business leaders in the US describe their biggest concern as "remote workers making choices that reduce security".

Cybercriminals, like all criminals, are opportunistic. They have taken advantage of this crisis and adapted in step with these workstyle changes. Last year in 2020, they more than doubled their attacks on web applications, targeted remote access devices, and preyed on remote workers' lax security practices to launch millions of phishing emails, often with COVID-themed content. Criminals also targeted critical networks that couldn't afford downtime, such as those of healthcare providers.

Motivated primarily by financial gain, cybercriminals are growing more sophisticated and posing a greater threat than ever in both the public and private sectors.

Phishing is a dominant threat

A significant spike in phishing attempts and BEC (business email compromise) is exposing organizations to fraud, malware and breaches. Criminals are harvesting credentials and gaining access to business systems by posing as known services in emails that link to fake login pages.

Criminals are also targeting businesses by using spoofing, credential theft, or impersonation to masquerade as C-level executives or finance department employees. They can then request information or payments from other employees by posing as a trusted entity, or attempt to make fraudulent business transactions. After gaining access to a high-privilege email account, they might also set up email forwarding to an imitation account to secure ongoing access to sensitive information, such as emails relating to finance and accounting.

70%

of cybercriminal activity now takes the form of credential phishing and BEC (business email compromise)

> **In 2019, BEC accounted for under 5% of complaints submitted to IC3 (the Internet Crime Complaint Center), but racked up $1.7 billion in losses–almost half of all financial losses recorded in their 2019 Internet Crime Report.**

Top 5 spoofed brands

According to Microsoft's Digital Crimes Unit:

1 Amazon	2 Apple	
3 Zoom	4 Microsoft	5 UPS

Top 10 targeted industries for BEC attacks

According to Microsoft:

01 Healthcare
02 Chemicals
03 High Tech & Electronics
04 Legal Services
05 Outsourced Services
06 Accounting & Consulting
07 Wholesale Distribution
08 IT Services
09 Real Estate
10 Education

Ransomware criminals are intimately familiar with the struggles IT departments face

- Microsoft Digital Defense Report 2020

The threat of ransomware is real and pervasive, and it doesn't stop at paying the ransom:

Criminals are savvy

The report makes clear that rather than relying solely on brute-force methodologies, attacks can be highly complex and the attackers several moves ahead of their victims.

The human threat

Human-operated ransomware attacks surpass the threat of malware and encryption. Criminals sweep the internet for entry points or enter networks via trojans. After gaining access, human operators make real-time decisions based on weaknesses in the victim's cybersecurity.

"The real damage is done when the cybercriminal exfiltrates files for release or sale, while leaving backdoors in the network for future criminal activity–and these risks persist whether or not the ransom is paid." - Microsoft Digital Defense Report 2020

"Microsoft's Detection and Response Team (DART)...has observed that ransomware continues to be the most common reason behind our incident response engagements from October 2019 through July 2020."

"Alert-fatigue"

The report notes that entire networks can sometimes be ransomed in as little as 45 minutes. Even when detected by antivirus and endpoint protection products, fast-paced attackers are often able to succeed due to “alert fatigue,” i.e. when SOCs and IT departments struggle to prioritize and respond to high volumes of alerts from various security platforms.

Aware of this weakness, sophisticated attackers often purposefully use off-the-shelf tools or well-known malware families, as these are typically categorized as lower priority than customized attacks.

RDP/VPN Remote Access Vulnerabilities

To enter a system, attackers may exploit a vulnerable interfacing system, weak application settings, or–in more than 70% of cases, according to the FBI–RDP (Remote Desktop Protocol) brute force. Attackers with access to administrative credentials are most successful. Credentials are often obtained through vulnerabilities in VPN and remote access devices.

"Ransomware attack patterns demonstrate that cybercriminals know when there will be change freezes, such as holidays, that will impact an organization’s ability to make changes (such as patching) to harden their networks. They’re aware of when there are business needs that will make businesses more willing to pay ransoms than take downtime, such as during billing cycles in the health, finance, and legal industries.”

- Microsoft Digital Defense Report 2020

The threat of DDoS (Distributed Denial-of-Service) attacks

DDoS attacks overwhelm an online application with internet traffic to make it unavailable to users, causing costly downtime. Besides creating disruption and potentially blackmailing the victim, the attacker often uses DDoS as a distraction from a more malicious underlying infiltration.

Inexpensive and uncomplicated to carry out, DDoS attacks are already popular among cyber criminals, but the pandemic has made the barrier to entry even lower. The surge in internet use caused by remote work and schooling means traffic is already high on many sites. It also makes it easier for the attackers to go unnoticed as they can blend with the regular traffic.

43%

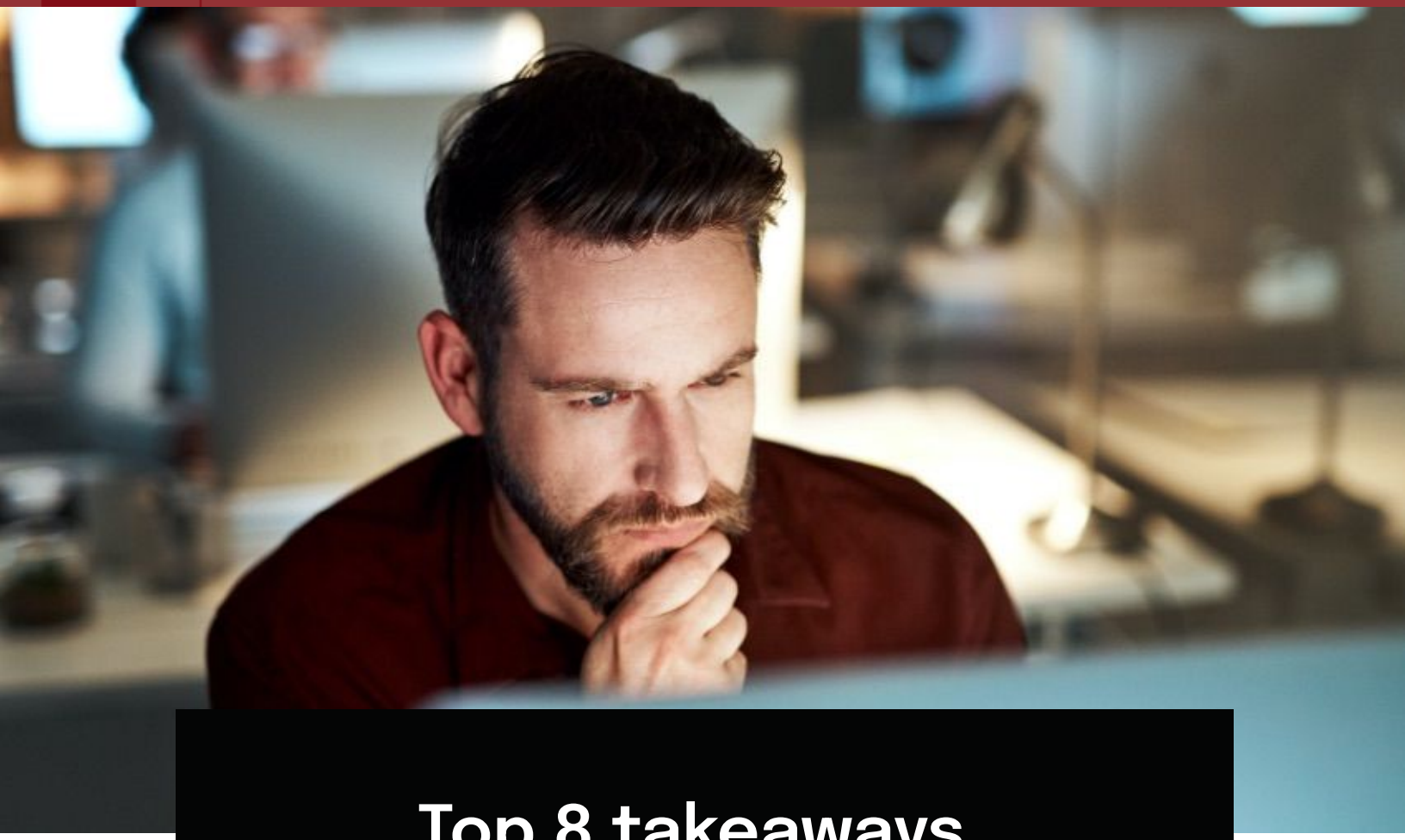
of DDoS were destined for distribution in the US

Microsoft recommends:

"In developing a strategy for DDoS protection, make sure your cloud and service providers' DDoS protection is enabled."

Microsoft observed a 50% increase in DDoS attacks in March 2020

> *DDoS attacks are some of the largest availability and security issues facing customers who are moving their applications to the cloud, making these attacks a significant concern for a remote workforce.*
>
> - Microsoft Digital Defense Report 2020



Top 8 takeaways

It’s a scary world out there.

To ensure your organization is safe, you should adopt all of the best practices laid out in the CIS Critical Security Controls for Effective Cyber Defense guidelines.

All organizations should adopt a security framework to minimize business risk. Umbrella suggests the Center for Internet Security (CIS) Critical Controls.

To help you navigate the complex world of cybersecurity we selected some of the most urgent best practices from the Microsoft Digital Defense Report.

01. Use Multi-Factor Authentication (MFA)

“Microsoft data indicates that the vast majority of Microsoft enterprise accounts that were compromised didn’t use multi-factor authentication.” - Microsoft Digital Defense Report 2020

Even if an attacker has your password, with multi-factor authentication in place they will not be able to enter your account without access to the additional factor–authenticator apps are safer than SMS or voice. This makes MFA the single best way to defend against credential-based attacks. While it is recommended for all users, MFA should be obligatory for admin accounts.

97% of credential stuffing attacks use legacy authentication

99% of password spray attacks use legacy authentication protocols

02. Practice good email hygiene

As the main gateway for attackers, email presents the greatest threat to your organization by far. To prevent phishing and other email-based attacks, you should practice good email hygiene. Disable auto-forwarding unless it is essential, use a platform that filters incoming mail and checks outgoing links once clicked. If you are using Microsoft 365, be sure to disable *Legacy Authentication*.

13 billion malicious emails blocked by Microsoft

1.6 billion were URL-based phishing threats

90% of all attacks start with an email

03. Patch your apps and systems

Updating your systems, Windows OS, Microsoft Office, and third-party applications regularly ensures you are protected by the latest fixes and security improvements, rather than leaving doors open for attackers. As well as closely monitoring your remote access infrastructure, you should investigate any security detections promptly, and reset all passwords on a device in the event of a compromise.

With remote work here to stay, your management strategies for hardware assets located outside of the corporate network need to be updated accordingly. This includes controlling settings and patching for mobile devices.

62%

of sites have unsupported Microsoft Windows systems, such as Windows 2000 and Windows XP, that no longer receive regular security patches from Microsoft, making them especially vulnerable to ransomware and destructive malware.

04. Take a 3-2-1 approach to backups

To ensure your organization's continuity in the event of a breach, you should prioritize backups using the 3-2-1 strategy, which dictates that you should have three copies of your data (the original, plus two backups) on two different storage types, with one copy off-site for swift recovery in the event of a disaster or breach. In an electronic world, this includes using a backup system that isn't reachable via your LAN and that runs on a different OS. For cloud storage, different accounts with completely different credentials should be used for backups, and immutable storage can be utilized to ensure the safety of your legacy files. This approach should also be applied to your SaaS providers, whose own backups may simply be stored in the same location as the primary data.

05. Use network segmentation

Segmenting your networks limits the spread of an attack and allows you to add stricter security controls on your most important systems and devices, as well as helping to defend unpatched systems.

54% of sites have devices that can be remotely accessed from internal networks by using standard management protocols such as RDP, SSH, and VNC, enabling attackers to pivot undetected from initial footholds to other critical assets.

06. Zero-Trust for remote access

Unmanaged devices, such as personal or BYOD, should be treated as untrusted. Any connection from these devices should be separated to an untrusted network with limited access.

Block direct access to Microsoft systems for unmanaged personal devices using Azure AD Conditional Access, and give users the option to enroll their device in order to gain access. Windows Virtual Desktop (WVD) can be used for unmanaged devices.

Azure AD's MFA capabilities can also be used to authenticate users trying to gain access to your organization's applications and infrastructure.

35%

increase in IoT attack volume from 2019 to 2020

07. Vet your supply chain

In an interdependent remote work landscape, supply chain security has never been more important. As seen in the recent SolarWinds supply chain attack, SaaS providers are being targeted as gateways into their customers' systems.

In light of this, you should vet service providers to ensure they follow cybersecurity best practices and apply least privilege access to your accounts and services. Third-party access to your network should be monitored and secured via MFA and just-in-time access.

Supply chain attacks are a small but growing threat, representing 7% of overall Microsoft Detection and Response Team engagement.

08. Focus on information rights management

The need for remote collaboration has necessitated access to sensitive data and intellectual property outside of the office. Enforce IRM policies for protecting documents and data, and to meet compliance requirements. Organizational data should be continually classified, labeled, and protected using encryption and controls that take into account who needs access and when.

In a recent survey conducted by Microsoft, 73% of CISOs indicate that their organization encountered leaks of sensitive data and data spillage in the last 12 months.

BONUS: Invest in continuous user training

Through training, you can turn users from your weakest link into your greatest security asset. Provide information on the latest threat developments, simulate phishing campaigns, build skills throughout the year, and develop a reporting system so that users can flag suspicious activity as soon as they notice it.

If you have $1 to invest in cybersecurity, invest in user training.

Contact Umbrella today for help with your cybersecurity

If you're concerned about the cybersecurity of your business, contact Umbrella to find out about our services. We can secure your systems and help you develop a comprehensive prevention and recovery plan that will ensure your data security and business continuity. Get in touch today for a free consultation.

The Umbrella Approach

Umbrella Managed Systems brings over five decades of collective experience delivering technology services and support. Unlike typical vendors, a personal touch is at the core of Umbrella's service model. We treat our clients like partners, and value long-term relationships with them. We work to understand our clients' goals and pain points, and we find solutions that not only fix today's issues but also deliver strategies for long-term success.

Contact Umbrella if you have any questions.

www.umbrella-ms.com

505 Walnut
Kansas City, MO 64106

816-437-7265