ActZero

Tackling Cyber Threats

IN A NEWLY DISTRIBUTED WORKFORCE

As organizations scramble to deal with the logistical kinks that come from hastily enabling a newly remote workforce to stay productive over months of lockdowns and travel restrictions, their IT teams must remain vigilant and flexible when it comes to securing tech assets amid changing circumstances.

They must help provide a cybersecurity backstop for personnel who are:

- Working from often insecure network locations
- Conducting business on more non-corporate owned devices than ever before
- Facing the distraction of new work-life balance issues

Attackers are targeting these unfamiliar situations and targeting new weaknesses in the corporate threat surface. They've brushed up on their social engineering of workfrom- home (WFH) victims, gone after consumer technology that's now linked to corporate assets and grown creative in how to take advantage of the explosion in collaborative software.

As a result, some 94% of security professionals agree that the COVID-19 crisis has increased cyberthreats to organizations.[1]

At the same time, economic conditions are more uncertain than ever. For the first time in many years, IT investments are expected to decline, with Gartner expecting an 8% downswing this year.[2] Security teams need to prioritize the most impactful threats targeting their newly distributed workforce without sinking a lot of capital expense into new infrastructure and in-house technology.

A changed risk landscape

Before digging into the most common threats targeting organizations in the quarantine era, it's crucial to understand the weaknesses attackers are most likely to exploit. The bad guys are taking advantage of a risk landscape transformed by rapid changes to technology and processes.

Remote work situations are hardly a new security consideration, but they've usually been more the exception than the rule—even within small organizations. The unexpected shift to WFH for most organizations has rapidly accelerated the scaling up of distributed workers. IT teams have been forced into a timetable for innovation that is difficult to stay ahead of.

As a result, many organizations have rushed to implement tools to support WFH, reducing the level of vetting and sound integration work normally expected of new technology rollouts. This has opened up a new field of vulnerabilities that hackers are already starting to exploit.

TechTarget | Custom Media

Additionally, businesses don't have control over employees' home networks, nor the personal assets connected to them, like Internet of Things (IoT) devices, which tend to be poorly secured. They may have been ignored by threat actors previously, but now they can serve as an entry point into networks now connected to corporate assets.

Meanwhile, back at headquarters, the network level security tools that IT teams previously depended upon to protect workers at the office—mechanisms like Network Intrusion Prevention (NIPS), gateway firewalls and sandboxes—are often no longer in play. Attackers are subverting them by targeting host systems and cloud resources that are separate from the network.

Understanding the threats

All of these risks are opening up the field for new ways to target employees and the organizations they work for. The following are some of the most common threats that SMBs and midmarket organizations should keep on their radar.

The rise of Zoom bombing
The use of web conferencing and telepresence software has skyrocketed. Recent figures show that in the first half of the year, the number of registered Zoom users more than tripled.[3]

Opportunistic attackers saw that surge as an opening for malicious activity, which was most dramatically presaged by the more mischievous and chaotic attackers.

The first signs Zoom was in the crosshairs came by way of unauthorized meeting joins. So-called Zoom bombs took advantage of configuration errors and nonexistent controls, or controls incorrectly set by administrators and meeting leaders who had little experience with the technology.

Businesses of all sizes must worry about how increased use of this technology is opening the floodgate for criminals seeking to profit off the new vulnerabilities introduced by remote meeting software. And there's no dearth of flaws surfacing. For example, a speaker at DEFCON this August blew the lid off numerous critical Zoom vulnerabilities,[4] and that was followed by unrelated discoveries in May[5] and July[6] of other core vulnerabilities.

Another weakness of unified communications (UC) tools that has yet to be discussed is the content of the meetings themselves. Recorded meetings are often full of personally identifiable information, intellectual property and otherwise valuable intelligence, which can be attractive to threat actors.

More potent phishing schemes
Attackers never let a good disaster go to waste. They're experts at developing social engineering ploys that resonate with the latest news cycles to trick people into clicking phishing links. The attackers have been taking full advantage of the pandemic, with COVID charity scams, fake infection maps, bogus personal protective equipment (PPE) sites and other schemes seeking to prey on users' fears and curiosity about the pandemic.

Spear-phishers are doubling down, not just on credential attacks but also business email compromise scams, including posing as vendors selling PPE to trick accountants and executives into wiring money to criminals, according to recent FBI warnings.[7] On top of that, attackers understand that SMBs and midmarket organizations are accelerating their move to the cloud. Attacks against Office 365 are up, and they're growing more sophisticated.[8]

More than half (53%) of cybersecurity pros say their organization has witnessed an increase in email phishing attacks since the start of the COVID-19 pandemic, and 30% of them report that phishing attacks have grown more successful during the pandemic.[9]

These attacks are growing more effective because it's more difficult for employees to be vigilant in the WFH era. The absence of offline ways to confirm if a manager actually did send an email is exacerbated by the distraction of balancing kids' remote schooling or a sick relative. Security awareness is more important than ever, but it's also challenging to implement remotely.

A ramp up in ransomware As a corollary to the rise in phishing, ransomware attacks are also up significantly. One recent estimate projects that there's been a 72% increase in ransomware since the beginning of the pandemic.[10]

Without the oversight they would have if employees were in office, IT teams are challenged to coach users and respond to requests that could help better protect end users from ransomware. Additionally, the blend of work and home life on both work and personal computers is increasing the risk profile for all devices that store or process business data. The cohabitation of people who work at different companies is also creating toxic possibilities for data exposure. In the past, breaches resulting from emailed exchanges of information between spouses have occurred,[11] but now there are potential new scenarios of interactions between spouses' corporate-owned assets—from two different organizations—that operate on the same network.

In the office, organizations normally take measures to ensure network-connected assets are protected. However, many employees running home routers themselves are a lot less likely to configure their networks with the same level of protection. Examples include enabling encryption, enforcing encryption key complexity or implementing access control measures, to name a few. Such networks are increasingly full of IoT devices that tend to have more vulnerabilities than typical corporate network assets. As a result, hackers may be reevaluating targets like these in the context of them serving as stepping-stones to corporate compromise.

Intensified insider threats
Companies have also lost many of the protections they once had to counter insider threats. Prevention controls and technology like data loss prevention (DLP) often don't work on home networks, and it's no longer possible to physically watch employees. Sometimes the biggest red flags for insider threats happen off the computer—people working in the office at strange hours or using externally connected devices. It's just not possible to watch employees the same way at home—not to mention having to navigate the swamp of privacy issues and liabilities unique to tracking employee behavior at home.

There are now many more practical WFH scenarios that can result in inadvertent insider threats. For example, an employee wants to work on a larger screen, so they move from a corporate laptop to a home desktop. And there are now new tactics that organizations can't control for, such as phones on tripods recording company data off otherwise locked-down corporate machines.

How to navigate WFH risks effectively and efficiently

The sudden shift to remote work and a completely distributed workforce has clearly introduced a complex set of new cybersecurity variables for under-resourced IT departments to contend with. Unfortunately, there's no easy answer—it'll take a layered approach to appropriately build coverage to match these new complexities. The following are some crucial ways to get started.

Fix visibility gaps
First and foremost, organizations need to fix visibility gaps caused by a rush to new technology, accelerated use of software as a service (SaaS) and increased tolerance of employee-owned devices. This means finding better means to keep tabs on endpoints and a centralized method for managing hygiene across the entire asset portfolio.

Keep security awareness top of mind
Find ways to disseminate and train employees on security best practices and the latest in social engineering attempts to fool them with phishing and malware.

Make sure incident response plans are in place
Backstop your security prevention and training with a solid incident response plan that's documented and tested to deal with the inevitable times that attackers still manage to break through defenses.

Leverage MDR effectively
Managed detection and response (MDR) makes it possible to contain and disrupt threats in a distributed environment without heavy investments in infrastructure. Organizations need a combination of proactive system hardening, vulnerability remediation, and detection and response capabilities to react to threats—but they may not have the resources to achieve such capabilities. With sensors that are operational in any remote environment, across multiple devices, and with actions enabled by endpoint detection and response technology, MDR services can thwart the spread of infection from an employee-owned device to other crucial corporate assets or networks.

MDR:

- Removes the onus from end users to report suspicious activity because the service's threat hunting team is detecting, responding and letting your IT team know what they did to correct it.
- Provides visibility into hygiene and reports on ongoing improvements thereto, prioritizing your efforts to correct issues.
- Enables your IT team to focus on its mandate: Deliver improved business outcomes through technological innovation.

ActZero

To find out more about how ActZero's MDR service helps to get in front of upcoming changes in the cybersecurity threat landscape, while reducing your security risk, click here.

To see our MDR service in action, request a demo here.

ActZero | ActZeroAI | ActZero.ai

www.ActZero.ai/contact

TORONTO
207 Queens Quay, Suite 820
Toronto, Ontario M5J 1A7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California 94025

SEATTLE
925 4th Ave., 20th Floor
Seattle, Washington 98104