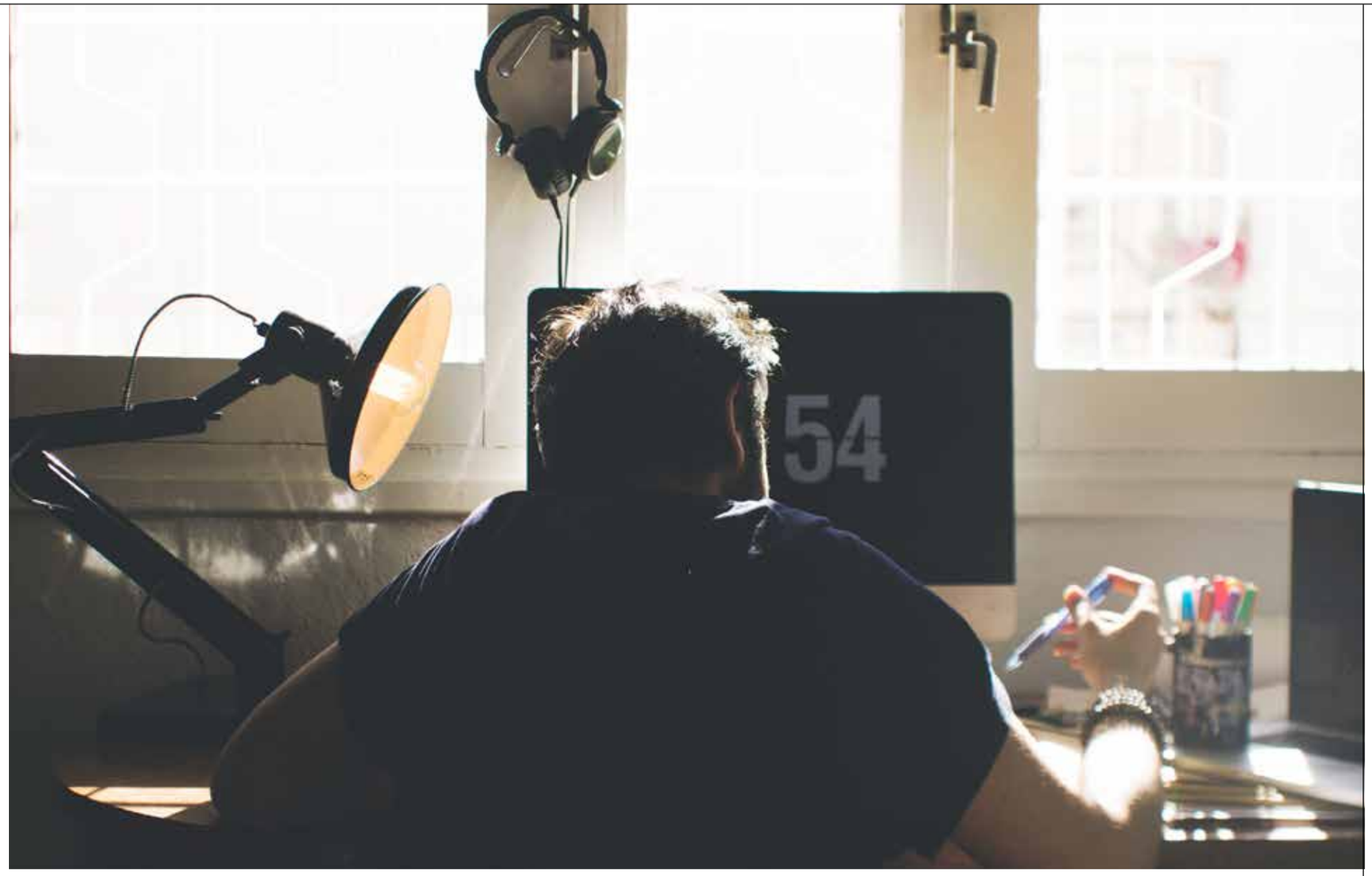
THE NEW NORMAL

Dave Waterson *on why the new hybrid workplace model presents a huge headache for security*



The risks associated with working from home have been well documented and from a corporate perspective, along with maintaining levels of productivity, perhaps the greatest risk of all has been the level of exposure companies have faced from cyberattacks when their employees are outside the perimeter of the corporate network.

In the months to come all indications suggest that companies hope to adopt a hybrid workplace approach, which will allow teams to spend some time in the physical office and some time working remotely. But what additional risks does this pose for those with security and IT responsibilities?

According to a survey of 2,949 employees carried out during lockdown by Atlas Cloud, almost three quarters (74 percent) of UK office workers said they wanted to be able to work from both the home and the office. This is not a surprise since so many companies prior to the pandemic were enabling staff to have the best of both worlds – the convenience and flexibility of home working and the collaboration and social benefits of the physical office space.

Enabling this hybrid workplace model will firstly require Bring Your Own Device (BYoD) and Bring Your Own PC (BYoPC) policies to be expanded and secondly a zero-trust approach to be taken to endpoint devices, such as laptops, tablets, home PCs and even smartphones.

NEARLY HALF OF UK BUSINESSES REGISTERED A CYBER BREACH OR ATTACK IN THE PAST YEAR

Securing endpoints has been one of the biggest headaches for security teams since March of last year – and, in fact, long before since 70 percent of all breaches originate at the endpoint, according to the Absolute 2019 Global Endpoint Security Trend Report. Insufficient protection on endpoints opens chinks in the corporate network, which elevates the risk of valuable data being stolen. It is all too easy for workers at all levels to be lured into opening links or attachments in emails, which appear to be from a reliable source but actually conceal malicious code.

Remote workers have also been targeted by cybercriminals through other members of their household, including children, to provide access to corporate networks. In addition, some cyber actors and advanced persistent threat groups have utilised pandemic themes, playing on people's concerns about their exposure to the COVID-19 virus through scams and phishing attacks. The problem has been so widespread that the National Cyber Security Centre reports that nearly half of UK businesses registered a cyber breach or attack in the past year.

While the risk of attack was intensified by the widespread location of employees, what we will face shortly as we come out of lockdown and start to adjust to the hybrid workplace, is that the devices on which employees rely will be used inside and outside the corporate perimeter even more frequently. Laptops that have been used on the previous day for a child's homework or to play a game will be subsequently connected to the company network, for example, and without protection they deliver a gateway for a cybercriminal to walk straight through.

BE PREPARED

Until quite recently, small and medium-sized companies, many of which are less thoroughly protected, were able to fly under the radar and dodge the kind of cyberattacks levelled at large multi-national corporate organisations. However, given the sharp increase in breaches across all businesses, this group is clearly also being targeted, and is often the least well-equipped to deal with the consequences. Smaller enterprises must act now and prepare themselves to armour business-critical applications and data against this increased level of threat. A cyberattack can be devastating, not only halting productivity, but proving financially costly if data is lost or stolen. Some organisations struggle to recover.

It is also important to learn from the experiences of others. When we were forced into remote working nationwide last year, many organisations believed that they and their employees would be kept secure by using a virtual private network (VPN) and an off-the-shelf anti-virus (AV) or an Endpoint Detection and Response (EDR) solution, but evidence suggests that this was not enough. A survey carried out by SentryBay last April among 1,550 British people working from home, found that 79 percent had been given additional IT software or security measures to protect their devices during lockdown. Of these, 56 percent had access to a VPN while 41 percent were given standard anti-virus software, but that didn't stop 42 percent of the total respondents receiving suspicious emails or 18 percent having to tackle an actual security breach. Interestingly only 28 percent said they'd been given protection specifically for the endpoints and applications they were using.

42 percent of people working from home in the UK received suspicious emails

So why are endpoint devices so vulnerable? Primarily because they are the access point that allows hackers and cyber-criminals to access the network. In addition they provide the attack vector – the keyboard and display – through which sensitive data is most frequently – and most easily – stolen. Along with spyware, keylogging malware, which monitors keystrokes on the keyboard, was last year ranked as the highest threat by the annual Global Threat Intelligence Report.

Part of the challenge for security teams is that despite the rise in use of anti-virus solutions, VPNs and even two-factor authentication (used most commonly in eCommerce scenarios) these solutions will not prevent an attack. In fact, if keylogger malware is installed on a remote endpoint laptop with a lower security posture than it would have in the secure corporate perimeter, an attacker could have full access as the user logs-in to *everything* the user enters at the keyboard or displays in a local application. Unless data is protected as it is entered from the keyboard or onto the screen – to protect against screen grabbing malware – it exposes gaps in the corporate armour to criminals who will not hesitate to strike.

Security teams must adjust their strategies to wrap their data and applications and neutralise the impact of information-stealing malware threats. To do this they must consider where threats begin and how they can be most efficiently stopped.

Kernel-level keyloggers, the most insidious form of keylogger attackers, harvest keys tapped on the keyboard the second they enter the operating system. Because they sit at a low-level, they are notoriously difficult to identify and eliminate, which is why they succeed against standard anti-virus solutions and can execute without being detected. What works to combat this threat are solutions that also operate at the kernel level, designed to protect the data being entered without relying on identifying and eliminating keyloggers. These solutions bypass any installed kernel level keyloggers, feeding false random data into the system while ensuring the real keystrokes are safely delivered to the application. They operate regardless of whether a keylogger is present or not silently protecting data.

Also vulnerable to threats is data entered into an application after login, or sensitive data displayed on the screen through the application. These forms of cyberattack include screen capture or screen grabbing, DLL injection and Man-in-the Browser attacks. Screen grabbing malware is often triggered to capture the screen when certain events occur, including the opening of a customer's account details for example, and this happens

perhaps every five or ten seconds while the target application has focus. The malware then covertly sends the captured screen images through to the command-and-control server of the attacker, where any data visually open on the image is stolen. Many companies are aware of the dangers of login credentials being stolen and advise their employees to use two-factor authentication, select complex passwords and update them regularly. Screen grabbing, however, if it can be executed, puts all information held within applications, as well as all information entered at the keyboard, under threat.

INSUFFICIENT PROTECTION ON ENDPOINTS OPENS POTENTIAL CHINKS IN THE CORPORATE NETWORK

Anti-screen capture mechanisms can be used to monitor and control screen capture APIs, which ensure that an attacker is presented with a blank screen rather than real data. Again, these solutions do not rely on identification and eradication of malware, but protect sensitive data regardless of the threats (known or unknown) present on the device.

Other threats while data is in the application are DLL injection and Man in the Browser (MiTB) attacks. A DLL Injection inserts malicious code into an application, providing access to sensitive data. MiTB attacks generally use java script code running in the browser, again providing access to malicious actors.

Typically, an anti-virus solution is used to guard against malware attacks, but for companies now embracing hybrid workplace models which put them at more risk, they will find more effective protection from containerisation solutions and secure, locked-down browsers. These prevent any unauthorised java script code or any browser extension to run in the browser preventing malicious activity. Containers are also a good prevention mechanism, allowing applications to be run inside a protected environment, ensuring only authorised code is running, isolated from any malicious code which may be present on the device. It is also useful to run a secure locked-down browser within a container, add kernel-level keylogging protection and anti-screen capture methods, to provide a secure environment on an unmanaged, remote-access device such as a home PC or personal laptop or any endpoint covered by a BYoD policy.

Cloud computing is now ubiquitous, but there is a risk while data (files being uploaded *etc.*) is being transmitted from the endpoint to the cloud from Man-in the-Middle attacks. Fortunately, due to the availability of effective solutions, these threats are relatively low and encrypted mechanisms are effective. But once data reaches the cloud for processing or storage, it can become vulnerable to cloud-based attacks such as APTs (Advanced Persistent Threats). These are sophisticated attacks which continue over a long period during which an attacker – once a foothold is gained – seeks to search and move around cloud storage setting up data exfiltration or denial of service attacks. DDoS attacks are a common occurrence and frequently make headlines and defence techniques, including containerisation and DevOps, are well developed and well documented.

With the array of threats laid out in this way, it is clear that cyberattacks are omnipresent and given the determination of malicious actors, can easily affect any company at any time with often disastrous results. The past year has been challenging for so many organisations, and with a further shift to manage in adopting remote and in-office working practices, security and IT teams have a hill to climb when it comes to protecting staff, corporate infrastructure and data. The key is to identify real-time security solutions that can easily create a seamless micro environment in which applications can run, data is protected and devices are safe both in and outside the network ●

Dave Waterson is CEO at SentryBay

IT security teams need to consider where threats begin and how they can be stopped