Digital Security
Progress. Protected.

How to plan a secure hybrid workplace

The Covid-19 pandemic changed the working habits of people all over the world, as well as the way we perceive workplaces. Experts agree that the future of work is hybrid, combining teleworking and standard office work. The new model might bring new challenges for IT admins. How do we create a hybrid workplace that is both safe and effective?

The hybrid office for hackers and cybercriminals who are constantly looking for ways to make use of the constant switching between company and private devices and networks. When not properly ready for the new model, small businesses may be endangered by various types of attacks. Here's what to watch out for if you want to keep your data safe and sound.

1: Create a new security strategy

New working conditions call for new rules. Now that you have a clearer vision of how the future of work looks in the long run, adapt your security strategy accordingly. Focus on both human elements and technology risks, including those connected to the usage of the cloud.

WFH and WFO

Shortcuts that stand for "working from home" and "working from the office." Even though the pandemic might be finally receding, teleworking is here to stay. According to a study conducted by the HR platform Hibob, during the pandemic, 63% of employees working full-time were working from home at least part of the time. Another study, introduced by McKinsey, confirmed that around 90% of global organizations will be combining on-site and off-site working permanently. This goes hand in hand with what employees wish for—as Microsoft suggests, 73% of employees want to stay flexible with working options.

If you want to avoid cyber threats, strategic decision-making and preparation are crucial. Your cybersecurity planning should be coherent, taking all potential weak spots into question. Such as:

- The human element. Employees may have adopted risky behavior as they started working from home, using home networks that are more likely to offer less protection from malware than company ones. Also, when working from home, employees become easily distracted and are more likely to click on malicious links. Cybercriminals can take advantage of this situation, targeting remote workers with more and more social engineering attacks. Therefore, it's worth reminding employees of crucial cybersecurity rules which must also apply for teleworking. Organizing regular training sessions pays off.
- Technology challenges. To give some idea of how the scale of attempted malicious RDP connections has increased, in the first quarter of 2020, ESET detected approximately 1.97 billion attempted connections. Just two years later, in the fourth quarter of 2021, about 166.37 billion connection attempts were made, which is an increase of over 8,400%. Therefore, make sure your VPNs, SaaS offerings and RDP servers are properly patched and configured. "They might become an easy target for cybercriminals, especially due to previously breached or easy-to-crack passwords," says IT journalist Phil Muncaster. IT admins should make sure that not only are company networks thoroughly protected, but also any hardware and software running on home systems.

Three principles of the Zero-Trust Policy

1.

ALL NETWORKS SHOULD BE TREATED AS UNTRUSTED

So should all your users. After all, you can't guarantee that an account hasn't been hijacked, or that a user isn't a malicious insider. That means granting employees just enough privilege to get the job done, and then regularly auditing access rights and removing any that are no longer appropriate.

2.

LEAST PRIVILEGE

This should include home networks, public Wi-Fi networks (for example, in airports and coffee shops), and even on-premises company networks. Threat actors are simply too determined for us to assume that there are any safe spaces left.

3.

ASSUME BREACH

Every day, we hear about a new security breach. By maintaining an alert mentality, organizations will be vigilant and continue to improve their defenses with a resilient zero-trust mindset. Breaches are inevitable—it's about reducing their impact.

2: Adopt the Zero-Trust Policy

What is the best way to manage the complexity of on-premises and remote workers and systems? How do you make sure that hybrid work and the prevalence of the cloud don't endanger company data? Adopt the Zero-Trust Policy. The notion is simple: No devices or users within the company network can be automatically trusted, and IT admins should not rely on the company perimeter security. Never trust; always verify.

All employees should have individualized access rights, devices should be regularly authenticated, access should be carefully managed, and network segmentation should be performed. Measures like MFA (Multi-Factor Authentication), applied to all accounts and devices, and end-to-end encryption, or network detection and response, will help you keep your business data safe.

3: Focus on an effective BYOD policy

Reduced hardware and software costs, convenience, and a sense of ownership. Those are some of the main advantages of the Bring Your Own Device (BYOD) policy, meaning that employees use their private devices for work purposes and use them in the office too. Nevertheless, when poorly secured, they might endanger the company network and data. As people return to the office, make sure they know how to handle cybersecurity, even on their own smartphones and laptops. Small businesses might address the challenges brought by the BYOD policy by improving their endpoint administration, e.g. a cloud-based dashboard that provides the ID admin with information about how many devices are connected to the network. Also, all mobile devices with access to company data and networks should be provided with a security app—no matter whether they belong to the employee or the company.

The hybrid workplace strategy in a nutshell

What measures should you implement if you want to protect your business?

- **Mandate the use of Multi-Factor Authentication (MFA) for all accounts and devices.**
- **Implement policies that require automatic updates to be switched on for all devices.**
- **Strong passwords for all home devices including routers.**
- **Psychometric testing to help identify where human weaknesses exist. This intel could be used to develop better security protocols and making training more personalized and effective.**
- **Strict vetting/auditing of suppliers and their capabilities for mitigating insider threats.**
- **Data loss prevention tools.**
- **Network segmentation.**
- **Restrict access rights via a least-privilege principle.**
- **Zero-trust approaches to limit the damage that can be caused by insider incidents.**
- **Modify working culture so those at home don't burn out on security practices.**
- **Audit the type of home security solutions being used by hybrid workers.**
- **Implement a cloud-based sandboxing technology which detects and analyzes never-before-seen threats to add another layer of protection.**

All in all, clever security solutions will help you turn your hybrid workplace into an environment that is not only motivating but also—and above all—comfortable and safe. It's never too late to start taking cybersecurity seriously. Now you know where to start.