The One Cybersecurity Risk You're Probably Not Even Thinking About



Printers may be the last thing on your mind, but they're a vulnerable point of entry.

April 4, 2019 6 min read

Opinions expressed by *Entrepreneur* contributors are their own.

In November 2018, people took to Twitter to post pictures of a bizarre message regarding a YouTube popularity contest. As it turned out, thousands of internet-connected printers across multiple countries had been hacked — each delivering the same unsolicited printout urging people to subscribe and spread the word about the YouTube competition.

The hacker who claimed responsibility for the stunt said he

was trying to teach people a lesson about printer security.

The incident showed just how easy it can be to penetrate a modern printer. Luckily, the hacker didn't have anything in mind more malicious than simply trying to increase a YouTube personality's subscription numbers.

Still, the hacker made a good point, because for most people, printer security is an afterthought; these devices might be the most overlooked high-tech item at businesses today. But the reality is that modern printers are powerful, network-connected devices which carry many of the same vulnerabilities – and liabilities – as any other network computer.

Related: Why Your Innocent Office Printer May Be a Target For Hackers

An overlooked security risk

According to a report by IBM Security and Ponemon Institute, the total cost from security breaches rose by more than 6 percent between 2017 and 2018. And that figure reflects how, for many organizations, exposure of sensitive information can be catastrophic.

Companies waking up to this danger might rush to reinforce workstation and network security while at the same time overlooking other connected devices such as … printers.

The problem hidden in an easy-access printer

By default, printers are typically set up for easy access and configuration on a corporate network. This default state may be convenient, but it also leaves printers vulnerable to outsiders – and not all hacks are harmless pranks.

A poorly secured printer can actually allow hackers to view

documents, steal intellectual property or other sensitive information, print anything they like or inject malware – potentially leading to even worse consequences down the road.

Fortunately, there are ways to manage your organization's printer security risks, and one of them might surprise you: a reliance on cloud services. Here are three strategies to help get the job done:

1. Trust the big names.

Storing potentially sensitive data in the cloud might feel like handing over your newborn baby to a complete stranger, but even the most reluctant old-school IT pros are starting to get it: Storing data in the cloud is more like keeping money in a bank rather than under your mattress.

This version of "the bank" may be less familiar than your bed, but it has vastly superior security and a team of people dedicated to protecting what's yours. Should something go wrong, the burden will not be on you.

As any CEO can attest, corporate cybersecurity is a complex and expensive war that never ends. Guaranteeing the integrity of data – to the greatest extent possible – requires significant resources and the best and brightest security technologists.

The major cloud application service providers are Amazon Web Services, IBM Cloud, Microsoft Azure and Google Cloud Platform – with AWS currently leading the pack on adoption rates, according to the *2019 State of the Cloud* report. Nobody is likely to outspend these companies on security-related technologies and methods, so that's where you should put your trust.

A private data center is a singular entity: a target with a location and IP ranges. But a secure native cloud platform

managed by any of these huge companies is not fixed to a location. It’s like spreading your data across multiple buildings far and wide, each with its own security measures right out of *Mission: Impossible*.

Related: 10 Ways to Keep IT Systems Secure

2. “Pack up” and lock down for your move to the cloud.

The transition to cloud services is easy. The process — connecting with your service provider and configuring your printing infrastructure with the cloud — happens in a matter of hours, often less. However, gathering information and *planning* for the move takes a little more work.

For starters, you should put a security policy in place for all network devices (including printers) and ensure that all employees are well versed in that policy. Last year, an independent review of the Kansas Secretary of State’s office revealed that two printers had not been properly secured, and neither was password-protected. During a penetration test, a security firm was able to infiltrate the entire government domain right down to the level of those printers.

Experience tells us an effective transition strategy must first plug such holes. It should also include configuring built-in device firewalls, shutting down unnecessary ports and protocols and developing a firmware-update schedule.

Related: 3 Simple Precautions for Protecting Your Personal Data in the Cloud

IT teams should further educate other employees to guard against attacks. If a hacker tries to infiltrate a company’s printer network and fails, other tactics may follow, such as email scams or other forms of direct contact.

3. Use security as a launchpad for more digital improvements.

By design, secure office printing is meant to simplify work for IT professionals: Instead of a company’s system having to manage multiple print queues and map employees to various printers, only one virtual print queue will be needed to serve everyone. And securing new devices in your environment can be done with a few clicks.

A study by Oracle predicted that by 2020, 67 percent of organizations will interact with customers through cloud-supported mobile apps, and 87 percent will deliver a multichannel experience. By shifting IT burdens to cloud services — especially in areas such as printing, which is not commonly the domain of in-house expertise — IT teams can spend more time focusing on core business operations.

When adopting cloud services, take advantage of all the new possibilities that not only protect sensitive information, but also ease the burden of routine maintenance and regulatory compliance.

For many organizations, their printing system is the weakest link in an otherwise reliable chain of security. The good news? It’s simple to reinforce. With some consulting and a little prep work, you’ll have the flexibility and freedom to focus on your core business while trusting the best-in-class cloud platforms to safeguard your data.

https://www.entrepreneur.com/article/331713