7 Security Threats You May Have Overlooked

Every time you fail to address a threat, you put the security of your network at risk. You've probably worried plenty about the downside: Confidential information finds its way into the wrong hands. Your network succumbs to a devastating hack. Customer data and customer relationships are compromised. Your stock and your brand value tank. Consumer goodwill seems irretrievable.
The cost to rise above and beyond a breach or intrusion is unknown (and possibly immeasurable). The trouble is: You may not be aware of all the threats to your environment.

This paper introduces seven often-overlooked security issues that threaten your network, your corporate data, and (by the way) your job. Here's a rundown:

1. Rogue employees may disable security settings to achieve individual productivity needs.
2. Confidential information is stored on personally owned devices, which leave the company when the employee leaves.
3. Your security solutions all come from the same vendor, opening up a single point of vulnerability.
4. Employees are running EOL software, and the vendor is no longer providing security fixes.
5. Your security solutions aren't adaptable to new technologies in your environment.
6. Your security solutions aren't flexible enough to uphold your company's security policies.
7. There's a disconnect between your security approach and the needs of the business, which may result in "Shadow IT."

1) Employees take matters into their own hands.

Much as you'd like to trust your company's employees to take security as seriously as you do, they won't always follow suit. Many threats are created by users who are unaware they may be opening a door for the hacker—either because they're naïve about security technologies or because they want to get things done as expeditiously as possible. Or both.

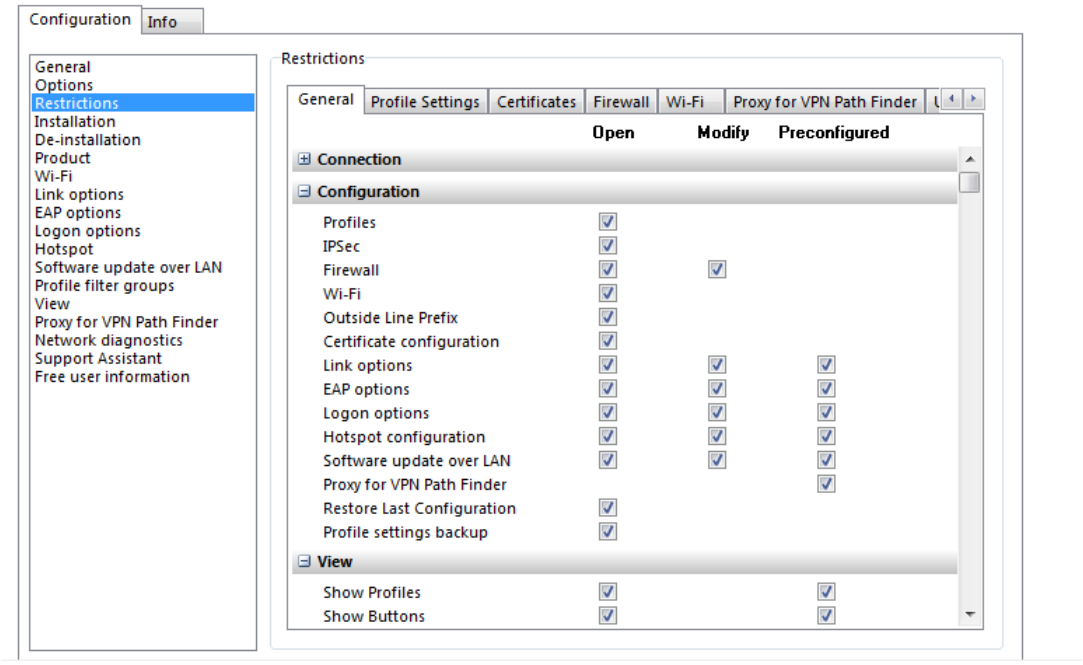
For example, you probably have users who take a company laptop home with them. If the end device (or end user) firewall is enabled, they're unable to print to their home printer. Without intending to endanger the laptop or the network, the user might disable the firewall. Or let's say you have mobile employees who work via VPN. You've configured their devices so that only Internet traffic via VPN is

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-100 · Fax +49 911 9968-101

allowed, but an employee wants to conduct some personal online matters outside the VPN, such as accessing resources on their home network or surfing the web. The user edits or changes the configuration of the VPN client so that online traffic is in the open.

In both scenarios, you can't blame employees for using whatever tools enable them to be more productive. But these rogue behaviors put the user's laptop at risk and may make it difficult to reconfigure the VPN or firewall. So they've not only raised a critical security threat, but also soaked up time and resources to fix the issue.

How do you prevent employees from taking matters into their own hands? While continuous training might help reduce these incidents, it won't prevent the problem. The more foolproof solution is to use centrally managed firewalls and VPN clients that don't allow users to enable, disable, or make changes to the software.



Parameter Locks for Users

2) Personal devices leave the company's control.

What happens when an employee leaves your company? Do they have a personal device that contains sensitive corporate data and network access information? A recent breach by a terminated employee of a Texas power company provides a good example of insufficient VPN management and security: The employee was able to use the VPN—even after his position was terminated—to access the company's consumer demand forecasts and to corrupt the data.

Employee termination procedures need to be adapted to the BYOD environment, with emphasis on security policies that are centrally managed and strictly enforced. The best approach is to connect user-provisioning and identity systems with VPN administration. By connecting your HR database with user-provisioning, you can make sure all access to corporate systems is denied from devices as soon as the employee is marked "terminated" in your HR database.

You'll also need a process for removing all company data from the employee's device. By implementing a mobile device management or container solution—which creates a work environment on the device—you'll have an easy-to-administer method of deleting all traces of corporate data and access information when an employee leaves the company. This approach also neatly handles situations when a device is lost or stolen.

3) Single security vendor. Single point of vulnerability.

The Heartbleed bug was a perfect demonstration of the widespread risk of embracing a single security technology. If your company relies on one vendor for all your security technologies—such as firewall, IPS, gateways, switches—you may have a false sense of security.

Let's look at a typical scenario. Your company's employees are connecting to the corporate network from a range of devices, locations, and connection media. A common approach to protecting their traffic is to deliver VPN services using a firewall as a VPN gateway. But since it's the same appliance providing the firewall and the VPN, both services will be affected if the appliance has a security issue. However, if you use one vendor for the VPN and another for the firewall, you're inherently adding a layer of security, because remote access to the corporate network must be authorized by two defense systems instead of just one.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-100 · Fax +49 911 9968-101

7 Security Threats You May Have Overlooked

If there's an overarching lesson to be taken away from the Heartbleed nightmare, it's this: No one technology (such as OpenSSL in the Heartbleed disaster) is guaranteed to provide comprehensive protection of sensitive data, corporate networks, and private communications. A multi-layered defense strategy—one that combines best-of-breed network and security components from a variety of vendors—can help you address many of the most common causes of a breach.

4) Employees are running EOL software.

The strategy "Never touch a running system" might be true regarding stability and productivity, but it may be wrong thinking when it comes to security. Since the vendor is no longer supporting an EOL product, they're also not fixing vulnerabilities that may be discovered.

Let´s take Windows XP as an example. Now that Windows XP has been EOLed, there's a persistent risk that an attacker may discover a "zero-day" vulnerability. If you have systems still running Windows XP — and in the absence of a Windows XP security patch — your network environment may be in severe danger. Keep in mind that zero-day threats exist with applications and other tools, as well as with operating systems.

How do you prepare and react properly to the risk of attacks on EOL products? Stay on top of all the operating systems and software your company's employees are running—and keep them up to date. Granted, it's a lot of work to implement operating system migrations and to discover legacy applications that don't run on a newer OS. However, a vigilant, ongoing approach to software updates is the only way to make sure you have trustworthy fixes to security vulnerabilities.

5) Your security solutions don't allow for innovations and new technologies.

Your computing environment needs to evolve along with the latest trends, tools, and operating systems. But what if your older security solutions are incompatible with advancing IT technologies? What if they don't support defensive measures against the latest security threats?

7 Security Threats You May Have Overlooked

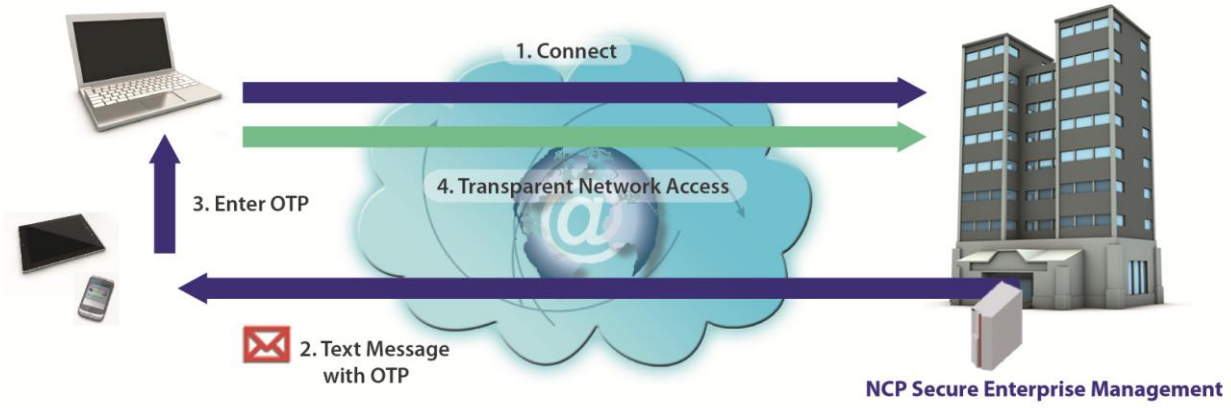
Make sure to build an intelligent, adaptable security solution that connects services from multiple vendors. New technologies like IF-MAP allow different vendor solutions to communicate and interact with each other, making it possible to react to threats with greater speed and flexibility.

Charles Darwin´s theory about adaptation is not only true for living organisms, but also for IT security: “It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.”

6) Your security solutions don’t match up with your policies.

There’s another concern around adaptability. What if your security solutions are incompatible with the security policies you’ve established for your company? What if they don’t include the features and functionality necessary to implement important security measures? Make sure to implement a flexible solution that supports the granularity of your security policies, procedures, and systems.

For example, some security vendors only provide user authentication via username/password, and do not support the use of certificates (PKI) or two-factor authentication (e.g., OTP or smart cards). If your company policy requires two-factor authentication, you’ll find yourself and your company at a dead end if your security solution doesn´t support it.



Advanced Authentication

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-100 · Fax +49 911 9968-101

7 Security Threats You May Have Overlooked

Another example has to do with your user directory. Perhaps you rely on an LDAP solution (e.g., Active Directory or Oracle LDAP) to provide a perfect digital picture of your enterprise based on users, group membership, roles, and other rules or flags. If your security solution can't identify users by the same rules, you may be forced to reverse-engineer your user directory to match the lesser functionality of your security solution.

7) Departments are procuring their own IT resources.

It's called "Shadow IT" and you've seen it in many forms. Departments may procure their own servers and storage systems. Maybe they outsource the management of their database or their data analytics. If you're not in touch with the business needs across your organization and you're not giving departments what they need, you run the risk of losing control.

How can you address the needs of the business without loosening critical defensive measures? Policy is key, and so is communication between security professionals and line-of-business executives. If you don´t communicate with company executives, you won´t be able to establish airtight IT policies. If you don't understand the needs of the business and its employees, you won't be able to enforce those polices.

Go ahead. Be a hero.

Information security professionals are modern-day gladiators, tasked with defending corporate data and networks against known and unknown threats. If all goes well, your efforts will go unrewarded—just as you hope you don't need to take advantage of your catastrophic health insurance or that $2 million liability coverage on your auto insurance. In the end, you'll be the preventer of that big downside risk—because you've recognized the threats and have taken steps to prevent them.

7 Security Threats You May Have Overlooked

About Julian Weinberger

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has ten years of experience in the networking and security industry, as well as expertise in SSL-VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP engineering. He also provides the company's key accounts with pre- and post-sales technical support for their remote access security solutions.

About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their secure remote access and to overcome the complexities of creating, managing, and maintaining network access for their staff.

Headquartered in the San Francisco Bay Area, NCP engineering serves 35,000+ customers worldwide throughout the healthcare, financial, education, and government markets, as well as many Fortune 500 companies. In addition, the company has established a network of national and regional technology, channel, and OEM partners to serve its customers.

For more information about NCP's remote access VPN solutions, visit www.ncp-e.com. You can also reach us on our blog, VPN Haus, or on Twitter at @NCP_engineering.

Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Phone +49 911 9968-100 · Fax +49 911 9968-101