KASPERSKY lab

IT & DATA SECURITY BREACH PREVENTION

A PRACTICAL GUIDE

Part 1: Reducing Employee and Application Risks

CONTENTS

AS CORPORATE NETWORKS INCREASE IN COMPLEXITY, KEEPING THEM SECURE IS MORE CHALLENGING.

With employees connecting to unsecured public networks and running multiple applications, sensitive corporate data is more vulnerable than ever before.

There's a lot to think about, and for your security policies to be effective, they need to bring all users and their devices under IT control and regulate employee behavior.

Though that sounds daunting, it could all be much easier than you think.
This guide is designed to simplify some of the issues and provide you with straightforward, practical tips that will help you protect your network and data, while giving your employees the knowledge they need to keep themselves—and your business—safe.

EMPLOYEES: IT SECURITY HYGIENE BEST PRACTICE

THE STORY

Thomas is the company CEO. He needs to stay connected, so as well as a laptop, he also uses his company smartphone and personal tablet for work.

Naturally, they contain sensitive information. He knows this needs to be protected, so he sets a password and a PIN - the same password he uses for his email and social media logins. The same PIN number he uses for his credit card. This is a typical example of “poor hygiene”. If just one of his personal accounts gets hacked, it could open the door to a critical loss of corporate data.

59%

of people fail to store their passwords securely

Source: Kaspersky Password Infographic

OVERVIEW

No matter what defenses you have in place, prevention is always better than a cure. And by making sure that all employees are taking basic steps to protect themselves, you can go a long way to reducing the risk of a security breach.

Something as simple as strong, unique passwords can make a huge difference. But we're all human. And even when we know we shouldn't, we're usually tempted to make life easier for ourselves. That's why 63% of us use easy-to-guess passwords, and 39% use the same one for all of our accounts. In other cases, employees may be unaware of the risks they're facing. Suspect links and unsafe email attachments may be an obvious danger to you, but the same isn't true for everyone in your organization.

That's why it's important to use both education and systems control to turn best practice into a security policy that's adopted and followed by everybody in the business.

> *"No matter what defenses you have in place, prevention is always better than a cure."*

PRACTICAL ADVICE

1

When it comes to passwords, you're in a position to control size, complexity and repetitive use. So use your policy to take away the temptation for employees to take shortcuts.

2

Make sure employees know the characteristics of phishing and potentially dangerous web addresses. Encourage them not to open links from unknown sources, to open any links they're unsure about in a separate window and to check URLs for consistency.

3

No one should be opening files from unknown sources, whether it's personal or work related. This should be a key element of your security policy.

TOP TIP: Passwords should be at least eight characters long and include upper and lower case letters, numerals and special characters.

TOP TIP: Before clicking through, employees should hover their mouse over links to check it’s leading to the site they’re expecting.

APPLICATIONS: MAKE PATCHING A PRIORITY

THE STORY

As you'd expect of any accountant, Maria's always busy. Especially today. She simply doesn't have time to wait for application updates to install. She hits "remind me later" and moves on to more urgent matters.

She's running old versions of Microsoft Office, Adobe Acrobat and most other applications she uses. But they work fine, so when reminders do pop up, she ignores them.

She gets through her hectic schedule and even manages to leave on time for a change. She heads home happy, unaware that the program she downloaded from a file sharing site earlier in the day was infected with malware, and that the malicious code has already exploited her unpatched applications and spread to the rest of the network.

49%

of people do not regularly patch or update software and OS

OVERVIEW

While it may not stop employees performing their day-to-day tasks, failure to update software increases the risk of a security breach. The majority of malware is designed to take advantage of vulnerabilities in applications. And the longer they're left unpatched, the longer cybercriminals have to exploit those vulnerabilities.

In fact, in most cases where attacks are launched through an application, a patch is already available. This is good news – it means they could have been avoided with relative ease. Consequently you should make sure that you're taking measures to find and deploy all available patches, and to remove the software you don't want or need from your network.

58%

of business have not fully implemented application control

Source: Global IT Risks Report 2014

PRACTICAL ADVICE

1

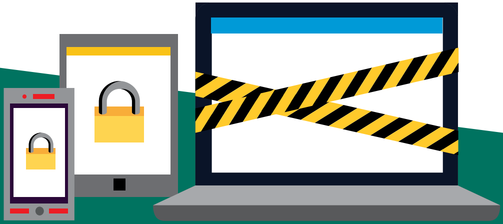
It's time consuming enough simply researching and prioritizing available patches, let alone deploying them. By using Kaspersky Endpoint Security for Business' vulnerability and patch management features you can automate this process, reducing both your workload and the risk to your business.

2

Give yourself the ability to spot and block unwanted applications and software that have found their way into your network. Kaspersky Endpoint Security for Business can give you both visibility and control of all software in use by your employees, helping you identify, register and track hardware and removable devices.

3

Give yourself the tools to enforce your application policies. With Application Control you can allow, block and regulate applications and using "Default Deny" controls, you can automatically eliminate certain applications from your network. Adding an extra layer of defense, Application Privilege Control monitors and restricts any applications that appear to be performing suspiciously. So, even if a program is compromised, you can still prevent it from executing malicious actions.



TOP TIP: You can disable the "remind me later" button, to ensure critical updates aren't ignored.

SUMMARY

Providing your business with the best protection possible requires a mixture of enforcement and education. Employees have more freedom than ever before – and that means they need to take more responsibility for their own safety than they may have done in the past.

That said, there's a lot you can do to eliminate opportunities for risky behavior altogether. And if you also have the tools to put your policies into practice quickly and easily, then you can spend less time reacting to problems and more time looking at the bigger picture, anticipating dangers and putting preventative measures in place before issues arise.

And that's really the most important thing—to be proactive. You already understand the threats you're facing. Now, using the advice in this guide, you can take practical steps to protect your business.

> *Employees have more freedom than ever before – and that means they need to take more responsibility for their own safety than they may have done in the past.*

PROTECT YOUR BUSINESS NOW.

GET YOUR FREE TRIAL NOW >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Visit Knowledge Center

Learn more at kaspersky.com/business

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com, to learn more about Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.

KASPERSKY lab

THE POWER
OF PROTECTION