IT & DATA SECURITY BREACH PREVENTION PRACTICAL GUIDE

A guide to reducing risk in today's IT environment

Empower business through security
kaspersky.com/business
#securebiz

KASPERSKY lab

IT & DATA SECURITY BREACH PREVENTION

As corporate networks increase in complexity, keeping them secure is more challenging. With users connecting to unsecured public networks and running multiple applications on both company-owned and personal devices, sensitive corporate data can now be accessed – and lost – from more endpoints than ever before.

There's a lot to think about, and for your security policies to be effective they need to bring every user's devices, applications – and even their behaviours – under control. More than that, they must be realistic.

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

CONTENTS:

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.

FACT

59%

of people fail to store their passwords securely

Source: Kaspersky Password Infographic

OVERVIEW

No matter what defences you have in place, prevention is always better than 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 organisation.

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.

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 programme 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.

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.

FACTS

49%

of people do not regularly patch or update software and OS

Source: Global IT Risk Survey 2014

58%

of businesses have not fully implemented application control

Source: Global IT Risks Report 2014

PRACTICAL ADVICE

1

It's time consuming enough simply researching and prioritising 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 defence, Application Privilege Control monitors and restricts any applications that appear to be performing suspiciously. So, even if a programme 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.

DEVICES: CLOSE THE DOOR TO MALWARE

THE STORY

Thomas has been to a conference. He's made a number of useful connections and is looking forward to going through some of the information he's been given on a USB drive.

As soon as he gets back to the office, he takes his MP3 player off charge, plugs the USB drive in and uploads the files onto the network.

With his mind firmly fixed on the opportunities that might come from the day's conversations, he doesn't stop to think what else might be contained in the files and clicks 'open'.

OVERVIEW

Just as URLs, files and attachments can be used to transmit malware, so can physical devices. Unless you check before opening, there's no way of knowing what a USB drive might contain. Even if it's company branded, that doesn't necessarily mean it's safe.

And it's not just USB drives that pose a problem. Any device that's been in contact with an unknown network could be infected. So, even if Thomas' USB drive is clean, the MP3 player he was charging could also pose a risk. In fact, removable media such as USBs and SD cards account for 30% of malware infections.

Again, there are automated steps you can take that will prevent your employees from doing risky things. But if they're also knowledgeable enough to exercise an appropriate level of caution, you can dramatically reduce the chances of malware finding its way into your network.

FACT

> "Removable media such as USBs and SD cards account for 30% of malware infections."

Source: Kaspersky blog

PRACTICAL ADVICE

1. Make sure employees check external devices and drives before using them, even if they think the source is trustworthy. Disabling auto-run can help and means they only open files they choose to.

2. Encourage employees to apply this same thinking to their personal devices too. For example, if they notice their smartphone is malfunctioning or suspect it might be infected with malware, they should know not to connect it to their laptop.

3. Using Kaspersky Endpoint Security for Business Device Control feature, you can specify the types of device that can connect to your network, and what they can do.

4. With the Application Control feature you can block malicious programmes on a device, even if they're opened.

TOP TIP

Set your anti-malware to automatically scan all devices and, based on the employee's needs, block any types of device that are unnecessary.

FACT

"The Stuxnet virus was initially delivered via USB to Iranian nuclear facilities, eventually spreading to Russian facilities in the same way. Malware has even made it to the International Space Station."

Source: Kaspersky Stuxnet press release

MOBILITY: PROTECTING EMPLOYEES, WHEREVER THEY'RE WORKING

THE STORY

Thomas needs to make the most of his time. So he uses his tablet to access his emails, as well as client data, when he's out of the office.

He finds himself with a spare twenty minutes between meetings and heads into a café to grab a drink and make some last minute amends to his presentation. He takes advantage of the free WIFI to send an email to his colleagues to make sure everyone has the latest version.

The file contains information he wouldn't want shared with his competitors. It doesn't occur to him that, by sending it over an unsecured network, he could end up doing just that.

OVERVIEW

With the rise of mobile working, it's no longer enough to apply security measures to just the hardware you have at the office. And since many employees 'bring their own device' (BYOD), it's not even enough to only protect company-owned devices.

While these working practices bring a range of benefits to the business, they also add extra complexity to your IT environment. And the widespread availability of free, unprotected networks – over which data can be intercepted – only adds to the challenge.

But it's not one you can ignore. Mobile should be a central part of your overall IT security policy. By being proactive you can help prevent data loss from sophisticated threats such as malware, and simple mishaps like losing a device.

FACTS

Almost

1/3 & 1/4

of businesses have experienced lost/stolen staff mobiles

of these know they lost data as a result.

Source: Kaspersky MDM Infographic

PRACTICAL ADVICE

1

If you don't know about a device, you can't protect it. Employees need to understand the importance of mobile security and of informing IT about all the devices they use.

2

Using Kaspersky Security for Mobile you can add anti-malware and other mobile security technologies to your devices and, with Mobile Device Management (MDM), you can oversee the administration of all devices in your network. As both mobile security and MDM are part of Kaspersky Endpoint Security for Business, you can integrate mobile security into your overall IT approach without any need for a separate, stand-alone solution.

TOP TIP

Make sure people understand that corporate data (including email) should only be accessed over a secure network. This doesn't mean that they can't make the most of free WiFi - just that they need to use a VPN.

TOP TIP

A lost device doesn't have to mean lost data. You can separate corporate data from the user's personal information. This sensitive data can then be encrypted, making it impossible to read if the device is stolen. You can then delete the 'corporate container' if need be – for example when an employee leaves the company.

FACT

"On unprotected WiFi networks all data can be intercepted and data on the screen can be modified. However, 34% of public WiFi users take no specific measures to protect themselves."

Source: Kaspersky BYOD Infographic

WEB AND SOCIAL: WHAT CONTROLLED ACCESS LOOKS LIKE

THE STORY

On her lunch break Maria takes a moment to check Facebook. She scrolls down her newsfeed and sees an interesting looking link. The article isn't what she was expecting so she shuts it down. The phone rings, she logs off and gets back to work.

Unfortunately the site in question launched a drive-by attack, and as she hadn't updated her browser since getting her laptop, she didn't get any warning that the site seemed suspicious. She had both her work and personal email up, and both have now been scanned by the malware, compromising important financial information.

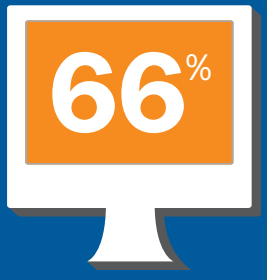
OVERVIEW

Much like BYOD, social media sites are another example of how intermingling our professional and private lives can have serious repercussions for online security. As well as being an opportunity for the spread of malware, they can help criminals collect information about potential targets.

It's important for employees to understand that, even if their browsing is personal, the risks can affect the entire company. By encouraging the right behaviours, you can implement a policy that keeps your network and data safe without impinging on the quality of employees' work life.

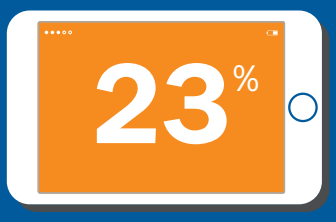
FACTS

Social media use is ubiquitous and spread across devices



of social media users access sites through computers

of social media users access sites through smartphones



of social media users access sites through tablets

Source: Kaspersky Social Network Infographic

PRACTICAL ADVICE

1

Tell employees they need to check the origin of anything they download and to hover over links to check the url matches the anchor text, especially if the site they lead to is unknown or untrusted

2

Make sure your policy covers employee conduct on social media sites. They should never share sensitive information, whether it's business related or personal. And they need to take responsibility for screening their contacts.

3

If sites are simply inappropriate for work, they should be excluded from your browsing policy. Using Kaspersky Endpoint Security for Business's Web Control functionality, you can use pre-set or customised databases to blacklist categories of websites that shouldn't be visited.

4

It can be difficult to spot some of the more subtle deceptions used to spread malware. Kaspersky Systems Management, which includes patch management, can help you ensure employees are using updated versions of their browser, reducing the risk of them running into trouble.

TOP TIP

Kaspersky Endpoint Security for Business has pre-built, customisable blacklists you can use to ban sites by type. As you can split users into groups, restrictions don't have to be company wide. If you're marketing team need to use Facebook but the rest of the company don't, you can make it accessible only to them.

FACT

The top three social media phishing targets are:

56% Facebook

8% Twitter

3% Pinterest

Source: Kaspersky Social Network Infographic

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 behaviour 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.

GET STARTED NOW: FREE 30 DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

#securebiz

Watch us on YouTube

View us on Slideshare

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

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 300 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.