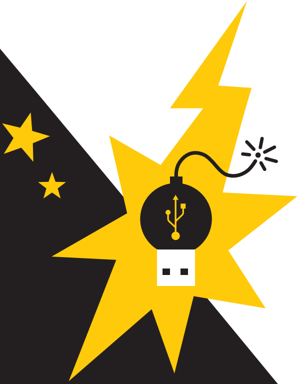
PAESSLER
THE NETWORK MONITORING COMPANY



SOMETHING LURKING IN YOUR NETWORK?

Get Control of Shadow IT

CONTENTS

1

LURKING IN YOUR NETWORK

Shadow IT – a concept becomes a household word. IT that is used outside of the official infrastructure of a company or without clearance from administrators is becoming more and more prevalent. From private smartphones and USB sticks to new cloud services, to private printers brought into the office: Shadow IT takes on many forms.

The issue, however, is anything but new. The question of what should or should not be allowed in a network has been around since the beginning of IT. So is Shadow IT just a fashionable term? No. Nowadays, it's extremely easy and inexpensive to subvert a company network, undermine it and thus put the entire company in jeopardy. The risk has increased drastically, and so has the IT department's need to take action.

Administrators must face the question of how to deal with Shadow IT. Before we continue: the simple method of exercising your authority and forbidding use of Shadow IT will technically work, but takes a lot of time and energy. We want to provide you – the administrators of midsized companies – with an alternative. Resolve the conflict between 'official' IT and Shadow IT. End the trench warfare and solve the problem for once and for all.

This ebook is for administrators as well as non-professionals. We avoid using technical terms so that any reader can understand just how important this topic is. The next time you have a conflict with one of your departments, share this ebook with the responsible persons. Maybe it can help to bridge the gap and help your departments to gain a better understanding of, and appreciation for, the issue.

2

4 EXAMPLES FROM THE SHADOW WORLD

#1 TOTAL FAILURE VIA FRITZ!BOX

A team leader in a mechanical engineering company had good intentions. He had a FRITZ!Box broadband router lying around in his basement and, because they often worked with laptops but didn't have Wi-Fi at the office, they built their own little network. The FRITZ!Box worked perfectly. So well, in fact, that it even functioned as an additional DHCP server for 2300 company computers, which led to conflicts in automatic IP address assignment. The result: most of the company was offline. The IT department searched for the problem for an entire day. This kind of complete failure can easily result in costs in the 6-digit range.

#2 HACKER IN THE CHAT ROOM

The new cloud service was promising. Internal communication should become significantly easier. Staff now communicated via an internal chat room and sent each other instant messages. It was very practical, as many details for projects could be discussed conveniently. One morning – about half a year later – the news spread like wildfire: the service had an open back door, and the data had been stolen and sold by hackers.

#3 THE CONTAMINATED USB STICK

“Another half hour and the presentation will be finished,” thought an employee of a medical engineering company. But she had a doctor’s appointment that she just had to get to. So she put the presentation on her USB and finished it from home that night on her personal computer. Little did she know that her computer was infected with a Trojan. The next day, she popped in her USB stick – and fed the Trojan directly into the company’s system.

#4 CLIENT DATA IN THE CLOUD

“This new CRM system is really practical. Everything is online in the cloud. We definitely have to try it out,” thought a marketing employee. So, he downloaded it onto his tablet. Three simple steps later, he’d uploaded an Excel table with client data to the cloud and breached data privacy laws. The next day, the employee worked late into the night with a bad conscience. He just couldn’t figure out how to delete the client data from the test account…

3

3 REASONS, WHY SHADOW IT EXISTS...

... and 3 Resulting Threats

IGNORANCE

Many employees are lacking basic IT knowledge. They don't see the consequences or the danger of their actions. They might be trying to avoid the effort of getting the IT department's approval.

GOOD INTENTIONS

The managers in the various departments want to use Shadow IT to accelerate or simplify their processes or reduce costs. They want to perform better. These are legitimate reasons.

NEW HABITS

Generation Y has reached the job market, and generation Z is close behind. Both generations are used to working with smartphones, tablets and laptops. They want mobile, flexible solutions.

INVASION/INTRUSION

Shadow IT is the open window on the ground floor – an invitation for break-ins. Employees' negligence endangers the entire company. Company secrets can be leaked or lost and data privacy laws are often violated.

DEPENDENCY

Shadow IT is like crazy glue on your fingers. With most external IT services, it's difficult to export data again. After a short time, a lock-in takes effect. If the service is changed later on – the prices raised, terms and conditions slacken or are removed completely – it takes a lot of effort to release your company from the service. You end up stuck in an unexpected dependency.

INEFFICIENCY

Shadow IT is like cable spaghetti. If each department creates its own IT solutions, chaos will soon ensue and will not be easy to untangle. Coordination becomes more difficult. Higher costs are accrued, as single IT solutions are implemented more than once without the departments even realizing that this is the case.

4

7 STEPS HOW TO GAIN CONTROL OF SHADOW IT

Most administrators have the same initial reaction when they discover Shadow IT in their company: they refer emphatically to the company's IT regulations. There are rules, and employees must follow them. After all, the IT department is responsible for ensuring that the data, network and all IT processes are secure and stable. If there's a data leak, the administrator takes the fall.

On the other hand: rejecting all new developments, like cloud-based services, doesn't make sense – even if they are located outside of your network. Administrators need to develop a cloud strategy.

Administrators should come up with a way to manage Shadow IT, so that it does not emerge underground again and again.

1

PUT SHADOW IT ON YOUR AGENDA:

Many administrators are drowning in everyday tasks. However, dealing with Shadow IT is part of strategic planning. Finding solutions for it helps to save time and effort in the long run. Put the topic on your agenda and actively communicate it on all levels in the company.

2

INITIATE THE CONVERSATION:

Explain what Shadow IT is to the different departments and ask your colleagues if and how they use it. Ask them why they use specific services or hardware. This will help you to identify weak points in your IT infrastructure. Create a report based on the information gathered to gain an overview of the situation and to make clear to company management how important the topic is.

3

CREATE A CODE OF PRACTICE:

Create a code of practice specific to your company that documents the responsibilities and standards. This provides the various departments with instruction for action, which, for example, can be given to new employees. The code of practice should be simple and clearly written. Offer accompanying presentations, internal workshops and/or a hotline.

4 OFFER ALTERNATIVES:

When an IT request is made, just saying ‘no’ doesn’t help. If, for example, introducing an external service is not possible due to security reasons, work together to find a suitable alternative. Do not leave your departments out in the cold!

5 CREATE INTERNAL TEST ENVIRONMENTS:

Is Shadow IT especially established in a specific department? There is usually a reason for it. The department might be especially driven in innovation. Create internal test environments especially for this department. Giving a “long leash” while maintaining clear guidelines is more helpful to you and the department than constant confrontation.

6 ACCELERATE DECISION-MAKING PROCESSES:

Every change in the IT structure must be checked carefully. However, companies today must be able to react quickly. The tempo has increased. Be systematic in your decision-making processes and identify areas where you can make fast decisions. Create a question catalog, for example, that you can distribute to the different departments.

7 STAY IN CONSTANT COMMUNICATION:

A code of practice is a good start, but it is just the beginning. Continuously pursue a proactive path. Don't wait until problems are springing up like weeds. Go to the departments regularly and ask them: what bothers you? What should be improved? In doing this, you help employees to gain a sense of the issue and, in most cases, they will come to you directly when they have a problem.

CONCLUSION:

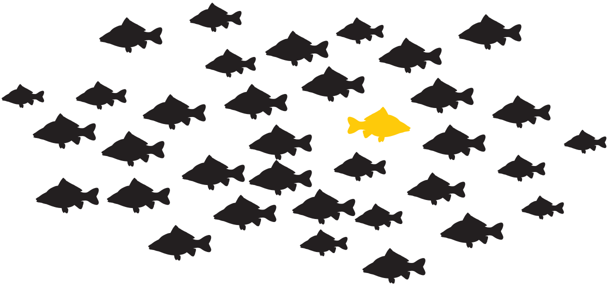
DEVELOP A NEW IDENTITY!

Become an internal consultant for productive work processes. Become a cross-department innovator. With IT that is perfectly attuned to employees' needs, there will be no need for Shadow IT!

5

1 MONITORING: HOW PRTG HELPS WITH SHADOW IT

Unfortunately, you cannot assume that every department will come knocking at your door to clear up all possible questions. Most departments are too independent for that. This is where PRTG Network Monitor comes into play. The monitoring solution monitors your IT infrastructure around the clock and notifies you of any problems, before they turn into emergencies.



With this monitoring, you will be able to identify whether you have a problem with Shadow IT, how big the problem is, and in which departments. Through continuous monitoring, you maintain a constant overview of the infrastructure. Here are three ways PRTG can help keep Shadow IT under control:

AUTO-DISCOVERY

Any new devices are discovered immediately, as soon as they are linked into the network. Read more about how to turn on Auto-Discovery here:

www.paessler.com/manuals/prtg/auto_discovery

MONITOR BANDWIDTH

Bandwidth monitoring enables you to identify how much bandwidth is being used, and which device or application might cause bottlenecks.

www.paessler.com/bandwidth_monitoring

FLOW ANALYSIS

Take a closer look at your traffic. Mails sent by spambots are instantly recognizable. File sharing and other methods are identified as well.

www.paessler.com/netflow_traffic

CAUGHT! NOW WHAT?

If you implement PRTG, it won’t take long for you to discover Shadow IT in your company. How do you want to respond when you ‘catch’ a department in the act? A word of advice: be tolerant. Don’t make a big deal out of their offense. Grant the department pardon.

Use Shadow IT to improve your IT! The department will thank you for it – and will be on your side in the future.

PAESSLER
THE NETWORK MONITORING COMPANY

100% NETWORK SECURITY!
SEE HOW PRTG NETWORK
MONITOR CAN HELP YOU:

www.paessler.com/
network-security-monitoring