Vulnerability Management

Automatically Detect and Quickly Eliminate Security Gaps

CONTENTS

1 Braving the Gap – No Chance!

Spectacular cyber-attacks in which thousands of data records are stolen or destroyed are making headlines, again and again. Those attacks are by no means the result of a stroke of genius from highly talented hackers. In fact, they are increasingly brought about by criminals who have managed to get through without expensive equipment and professional programming knowledge. They use exploits available free of charge online for many thousands of vulnerabilities that are potentially present on every Windows client and server in a company. A successful attack can be led through each of these gaps. Firewalls and virus scanners do not offer effective protection against these kinds of attacks. It can also be dangerous when a device is not securely configured – a password that has been reused over many services makes attacks on your activities needlessly easy.

Braving gaps is not a virtue for IT administrators against this backdrop. Instead they bear responsibility for the security of data and disruption-free operation of infrastructure. Customer data, business figures, development documents – the consequences of a successful cyber-attack can paralyze operation and disclose confidential company information. In addition to financial losses and damage to the company's image, in the worst-case scenario there is even the risk of investigations by state prosecutors, for example if an infringement of data protection laws is suspected, or if company computers seized have been connected to a botnet and controlled remotely to carry out cyber-attacks. In this case, the trail of IP addresses will lead back to the company.

The high and constantly increasing number of security gaps means it is just not possible for an IT administrator to maintain an overview and reliably ensure the greatest possible degree of security on all end devices without automated resources. The same goes for the configuration of many devices in a business. This white paper describes what dangers are out there and how to design automatic vulnerability management using an endpoint management software, in order to reliably detect dangerous gaps and quickly close them.

2 From Vulnerabilities to Cyber Attacks

2.1 Definition: Vulnerability, exploit, and co.

A vulnerability is like a window you forgot to close in your house: it represents a security-relevant error in an IT system or an institution. There is therefore the potential that a crook could break in – but this is not absolutely guaranteed. However, it would be careless to leave the window open for longer than necessary.

It would be dangerous if there were an exploit for the vulnerability – an appropriate tool for exploiting the gap. Then the crook has the ladder in their hands, which they can use to reach the open window. So, while a man in dark clothes with a robber mask and aluminum ladder in the neighborhood could attract attention, exploits can be easily and mostly anonymously downloaded from the Internet. In the meantime, an entire underground industry has developed, which survives on earning money through exploits. Payment is simply through services like PayPal. There are even free exploits available.

Exploits are used to smuggle what is known as the payload into the system being attacked: a popular malware program that spies out data, deletes files, or makes the endpoint part of a botnet – in other words, the sack which the burglar uses to stash and carry away their haul.

A framework like Metasploit, which was actually developed as a tool to detect security gaps, also enables users with a bit of experience to use exploits and run attacks. Metasploit is simply installed on Windows or Linux, has a menu-controlled or graphical user interface available and is also available as a virtual machine. And if that's still too complicated, help can be found in Internet forums or YouTube quick guides. Potential hackers therefore have a tool that is as easy to use as a ladder, but much less conspicuous.

2.2 The lifecycle of a vulnerability

Software is a highly complex product: according to Microsoft, Windows 7 for example was made up of some 40 million lines of program code. As a rule, good software contains less than one error per 1,000 lines of code. So even with the best quality controls, enough gaps remain open that can all develop into a problem for IT security.

While the vulnerability is lying dormant in the shadows, the risks are low. However, things look quite different when the open window catches someone's eye – whether a developer, a security expert, or an amateur programmer. These people communicate with each other in Internet forums, document vulnerabilities identified in databases, and report them to the software developer. Large companies such as Microsoft or Google pay bonuses for new gaps that are detected, so as to be able to close them quickly.

Generally, it doesn't take long for an appropriate patch to be available that closes the gap. But that doesn't mean the danger is eliminated – quite the reverse! Exploit developers also read vulnerability databases to find out about gaps. They analyze the patches provided by the developer and from this can draw inferences as to how they can exploit the gap. So long as the patch has not been installed on all of the devices affected by the gap, effective attacks are possible by exploiting the known vulnerability.
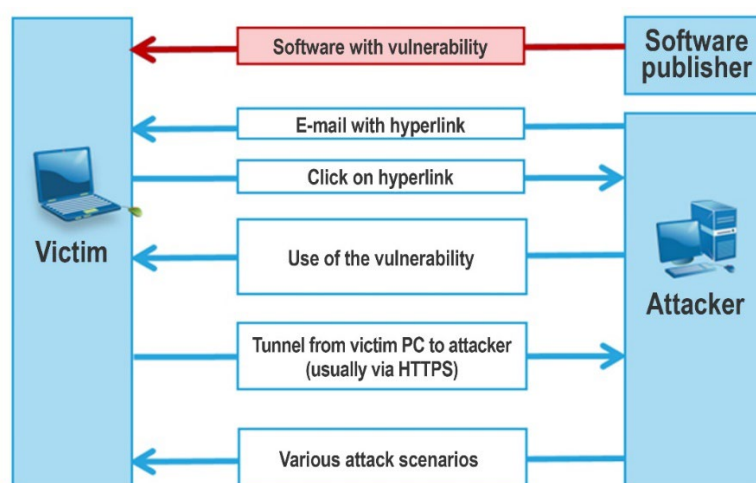
| Vulnerability exists | Vulnerability detected | Patch provided | | Patch installed: secure system |

Risk until the gap is closed on all devices

2.3 Attack vectors: How to handle attacks on your firewall

In the past, cyber criminals generally tried to remove the firewall, and thereby gain access to the network behind it. However nowadays security precautions are so sophisticated and effective that this method generally fails.

Today's online hoodlums opt for more subtle methods. Sometimes attacks are through displaying websites that are actually harmless. Or the hackers lure their victims to primed websites that deploy malware code. Manipulated files, which exploit vulnerabilities in display programs (DOC, PDF, etc.) that users install, are also used. Hackers use information from social networks and similar sources to trap their targets.

A classic example: An email to the employees of a large company with a subject heading that promises sensational discounts for a popular product. Without a doubt, a certain percentage of recipients will click on the link in the email. But what opens is a fake webshop, which targets a vulnerability in the browser or flash player. The user gets annoyed at the website which repeatedly fails to load correctly, closes the window – and certainly won't let the administrator know, as private surfing is forbidden at work.

Possible attack scenario through a software vulnerability

If the security gap exists on the PC where the link was clicked, it is already too late ... the attack succeeded. Now there is malware on the computer, which contacts the hacker. As this connection was established from the company network, the attack cannot be detected by the firewall.
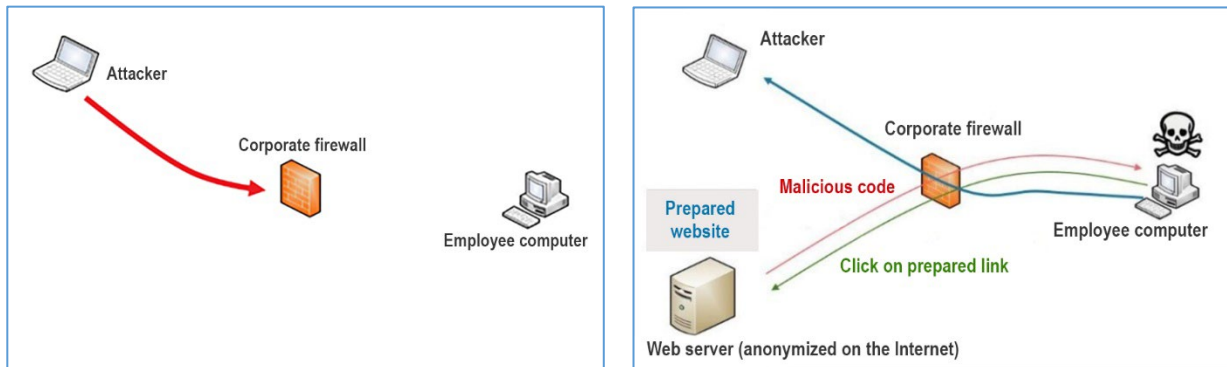
Connection set-up to the attacker

A good firewall, effective anti-virus software, and management of user rights are therefore still essential. However, they must be extended through further measures: by raising the awareness of all users. And in particular, through closing all security gaps consistently and as fast as possible on all devices.

3 Identifying and Closing Vulnerabilities

3.1 Impractical: Manual vulnerability management

In practice it is well-nigh impossible for an administrator to manually sound out all PCs, notebooks, and servers in their environment for all known vulnerabilities. In the last three years[1] alone, more than 80,000 new security gaps were registered in the National Vulnerability Database[2] – around 550 a week. To this we should add gaps that have been known for a long time in programs that are still used, combined with different language versions, and if necessary operating systems and process architectures.

The administrator has to continuously search databases and blogs for reports of vulnerabilities, evaluate said vulnerabilities, check their computers, package, test, and deploy updates, and record whether deployment was successful. In larger networks and companies split over several sites or with field employees, this approach is doomed to failure. At the same time the IT director must also guarantee the environment's compliance, be able to report the patch status if necessary, and in extreme cases take responsibility for problems.

3.2 Automatically trace security gaps on every endpoint

There is the option of using automation tools, such as the endpoint management software baramundi Management Suite. This solution continuously scans the endpoints and servers in the environment for vulnerabilities and gives the option to quickly and centrally close gaps. Both devices connected in the company headquarters and end devices in external sites or belonging to field staff (or in a home office) are considered.

To do so, the system accesses the constantly updated vulnerability databases of reputed organizations. The vulnerability scanner in the barramundi Management Suite uses a catalogue of known vulnerabilities in order to detect security gaps in the IT environment. A clear overview is provided by a dashboard, which shows administrators the state of their environment. List displays allow administrators to drill down by computer, vulnerability, or threat level: allowing them to target identification of devices with the most security gaps, the most vulnerabilities in the environment, or the most dangerous gaps, in order to resolve them as quickly as possible.

---

[1] January 2017to December 2019
[2] https://nvd.nist.gov
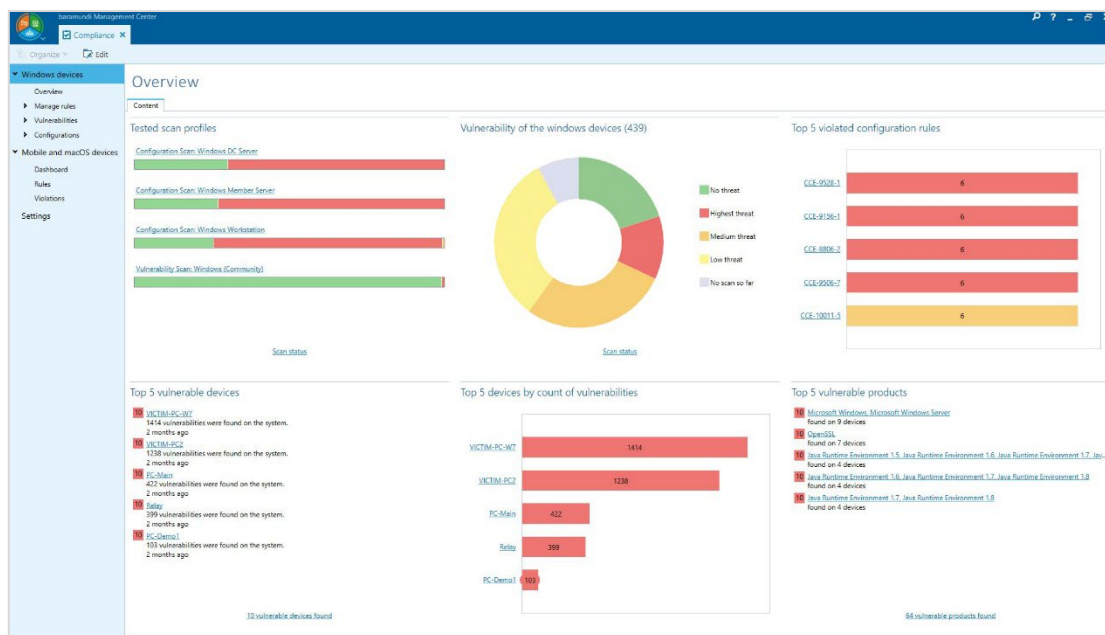
baramundi Management Suite: Overview of the threat to the environment in the compliance dashboard

This vulnerability scan takes place in the background using minimal resources, and does not impact the work of users logged on to the endpoint. At the same time, it gets ahead of potential hackers: administrators receive all necessary information to close existing gaps as soon as possible before they can be used for attacks.


Vulnerability exists

Vulnerability detected

Patch provided

Patch installed: secure system

Fast installation of the patch reduces the time period marked in red, during which attacks are probable

3.3 Closing security gaps centrally and automatically

In order to deploy the necessary updates and patches, the endpoint management software also offers automated solutions. Updates for Microsoft products are provided via a patch management module that supplies computers with all necessary updates based on a set of rules. The installations run in the background and any reboots required are combined in order to minimize installation time. And because patches can be installed from multiple file servers, the network load remains low. Administrators release patches automatically or manually, and define different rules for different groups. Following the introduction of cumulative patches from Microsoft, it is possible to roll out the functional and security-related updates to the endpoints and servers bundled together.

Program updates for non-Microsoft products are also provided by other software publishers (e.g. Adobe, Mozilla) as deploy-ready software packages, which can also be used for initial or uninstallations. The endpoint management software also takes on automated deployment – even to external sites that are only connected via the Internet, or to the notebooks of field staff.

As all processes in the endpoint management suite are connected, IT administrators receive meaningful feedback on all processes: successful installation, installation in progress, errors occurred – this ensures that the security patch is not just sent on the trip, but that it also reaches its goal and closes the gap.
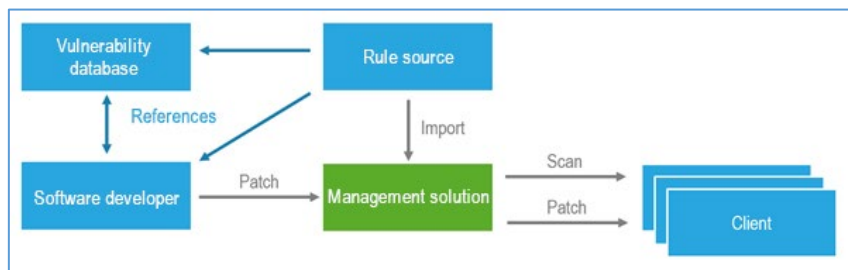
Importing rules and patches, scanning endpoints for gaps, and central patch deployment
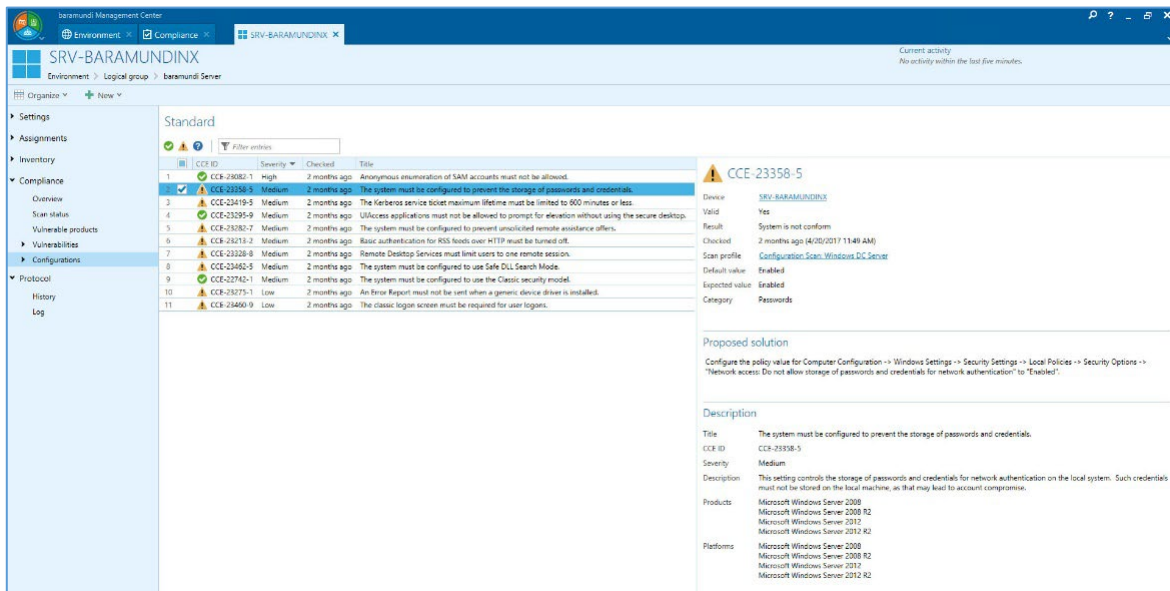
4 Configuration Management

4.1 Enforcing Secure Settings

Password length and password request after an idle period – these kinds of settings are essential for the security of a device. It is also important to learn whether AutoPlay is disabled for all drives, which kinds of remote access on remote computers are possible, or whether a reversible password encryption is permitted.

These types of settings are generally deployed and specified according to group guidelines. However, to enforce a high level of security, it must also be checked that these appear on all endpoints. It is possible that the configuration has been changed in the framework of support measures or by the end user without authorization to do so.

However, just as when searching for vulnerabilities in applications and operating systems, it is realistically impossible for an IT administrator to keep an eye on the configuration of every computer in larger environments without an automated aide. A solution for configuration management remedies this. This checks a standard rate on endpoints that reflects the company-internal requirements of the configuration. Such solutions – often bundled with solutions for vulnerability management – are offered integrated into endpoint management systems.

Result of configuration scan on a Windows client

They clearly show the IT administrator which devices are exhibiting infringements. The results of the scan can be displayed for the individual endpoint or aggregated at the level of groups and/or organizational units. Solutions will also be suggested to fix any infringements in a targeted manner.
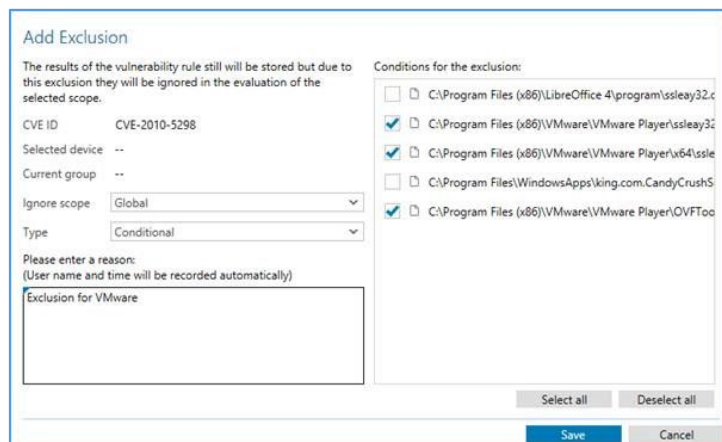
4.2 Exceptions prove the rule

In a complex IT environment, the software used is usually very diverse. Different applications of standard software, special custom software and/or various operating system components are located on the end devices in the enterprise. This software in turn includes isolated components (e.g. SSL libraries) that could contain vulnerabilities.

As a user, you can usually not replace these libraries in isolation without getting an update from the program publisher. If the affected programs are dispensable for the company, then uninstalling them may be the method of choice. Otherwise, a risk-benefit assessment may also lead to the decision to continue to use the program, and the OpenSSL libraries in the program directory are declared as exceptions.

For good vulnerability management of an endpoint management solution, it is essentially in this case firstly to ensure transparency that a potential security gap may exist and secondly to offer the option to define exceptions that deliberately display these vulnerabilities and tolerated exceptions within the company.

In the example below in the baramundi Management Suite, the vulnerable library is tolerated in the context of the VMware Player according to an exception rule, whereas the same file is not accepted for LibreOffice or other programs.


Define exceptions for vulnerabilities

5 From Vulnerability Management to Endpoint Security

Automated vulnerability and configuration management is an effective component of a successful security strategy. However other aspects also have to be considered for high endpoint security and data security.

Security gaps on smartphones and tablets that are now found in almost all large networks must be detected in order to quickly introduce countermeasures. For mobile devices, this kind of scan is at least as important as on PC clients, as consumer-oriented mobile devices generally do not provide for an administrator role which could enable an end user to prevent a software installation. For this too there are automated tools available, for example baramundi Mobile Devices which is integrated in baramundi Management Suite. It checks freely definable rules on managed mobile devices and detects things like jail breaks, root attacks, or undesired apps.

Further endpoint management software solutions allow data and user settings to be centrally and automatically backed up, encrypt mobile data carriers (e.g. USB sticks), prevent illegal copies on mobile storage media, or block – by means of app blocklists and allowlists – the start of unknown, unauthorized applications in the company network, effectively supporting the administrator in guaranteeing the best possible level of security.
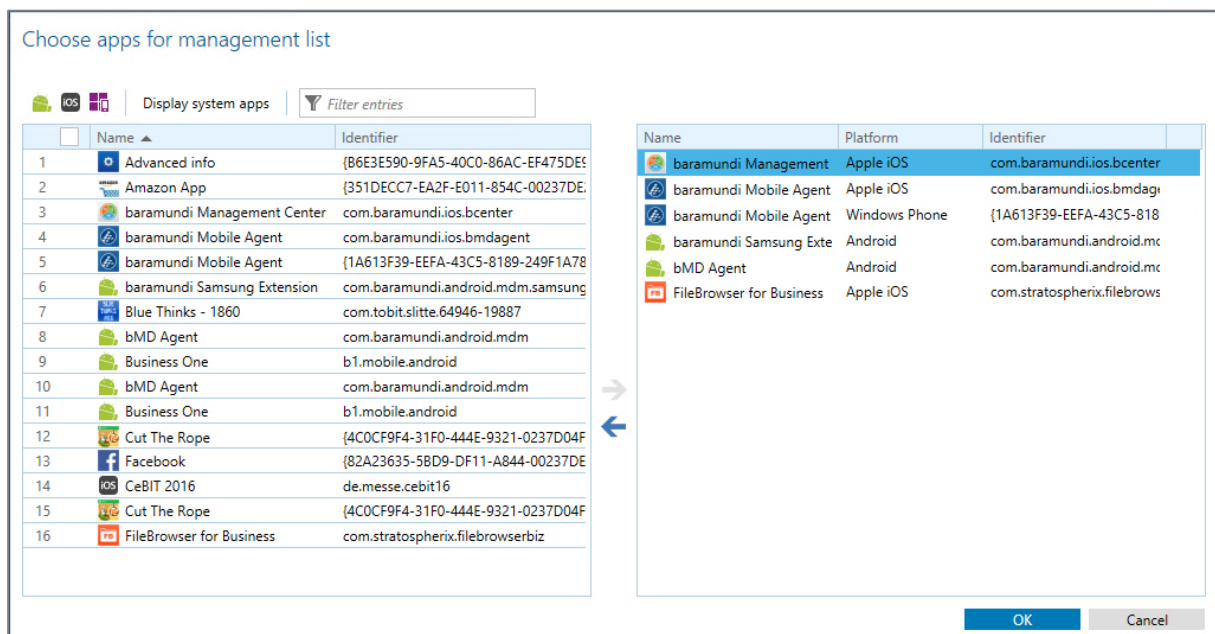
App-Block- and Allowlisting

About baramundi software GmbH

baramundi software GmbH provides companies and organizations with efficient, secure, and cross-platform management of workstation environments. Around the world, over 4,000 customers of all sizes and from every sector benefit from the German manufacturer's many years of experience and outstanding products. These are compiled into an integrated, future-orientated unified endpoint management approach in the baramundi Management Suite: endpoint management, mobile device management, and endpoint security are provided via a shared interface, using a single database, and according to global standards.

baramundi Management Suite optimizes IT management processes by automating routine tasks and providing an extensive overview of the status of all endpoints. It relieves the pressure on IT administrators and ensures that wherever users are located, they always have the necessary rights and applications on all platforms and form factors, whether on PCs, notebooks or mobile devices.

baramundi software GmbH is headquartered in Augsburg. The products and services of the company, which was founded in 2000, are fully Made in Germany. baramundi successfully works with partner companies around the world in sales, consultancy, and user support.

You can read various user reports by baramundi customers here. For more information, please visit our website www.baramundi.com.
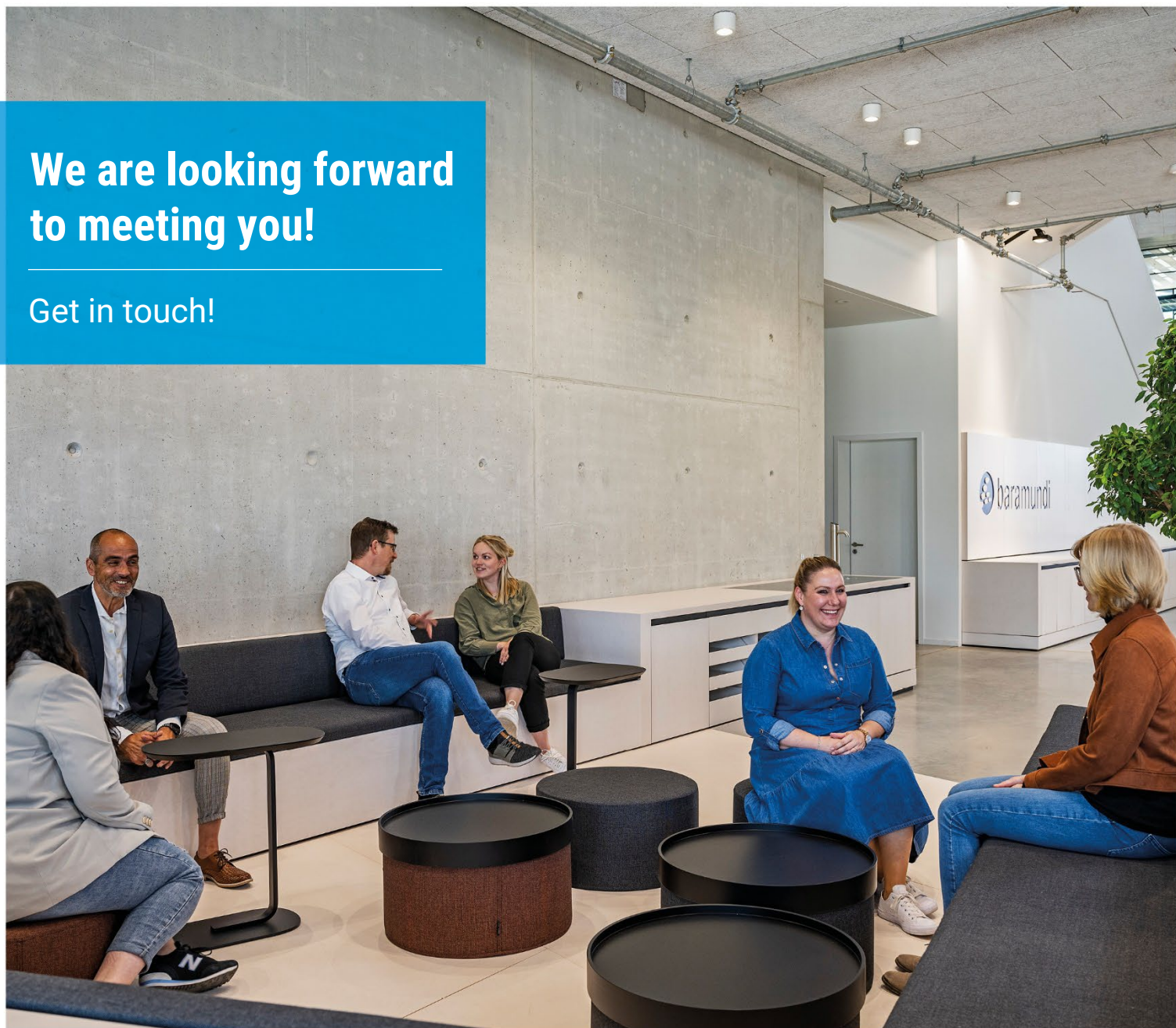
You want to learn more about the baramundi Management Suite? Register for the live webinar!

Discover cross-platform management for PCs, servers, mobile devices, Macs, and virtual environments by using the baramundi Management Suite in a free webinar.

www.baramundi.com/it-training/

We are looking forward to meeting you!

Get in touch!