ROLKEN

Resilience, Reliability & Security

Rolken s.r.o.
Nademlejnská 600/1
198 00 Prague 9

+420 228 224 645
hello@rolken.cz
rolken.cz

Table of Contents

OVERVIEW

For 15 years we have been providing our services in the areas of cyber and IT security. From basic vulnerability scans (where you tell us what we can do for you) to security transformations (where we tell you the possibilities and how to proceed). This is the work we do **for industrial** and **regulated organizations** as well as for **large companies**.

The outcome of our work is **an increase in the resilience and security** in all areas of your operation. We are able to accomplish this by **applying our expertise and know-how** from all different fields.

The numbers speak for themselves: **97% of** our projects are completed **on time** (within the confines of budget and project specs); **99%** of our clients are satisfied with **the quality we provide**; we can boast **98%** customer **satisfaction**. We cooperate with **90%** of our clients on a **long-term basis**.

We were formed in 2013 as an spin-off of SUNFLOVV, a company which from 2007 provided services related to information security and security outsourcing, and namely, without ties to security products or providers.

We do not have any outside investors. Our company is located in Prague and is employee-owned. Since the beginning we strive to uphold principles of a **distributed company** with a focus **on technology, innovation, and automation**.

WHAT WE CAN DO FOR YOU

It was not merely a better engine that made it possible to create the Shinkansen bullet train, but better breaks that allowed for harnessing the power of the engine. And this is our philosophy as well – in order to go forward quickly, you need to have the ability to break.

IT AND OT ASSET MANAGEMENT

Having a list of your assets – system types, applications, hardware, active firmware – is the absolute starting point for security solutions. Because how can you protect something which you do not even know exists?

We will help you to develop a process, set up a system and automate it as much as possible, so that you will have all the relevant information regarding your assets and the state they are in.

RELEVANT APPLICATION

If you only do one thing to safeguard your security, then make sure it's the managing of assets. Without a current list of your assets, each additional measure or step will have either a decreased effect or none at all.

OUR PROCEDURE

We will create for you a list of assets – hardware, software, apps, firmware, frameworks – in short, any and everything that we find. We combine technical data from probes and scans along with inventorial and other "paper traces."

RESULT

You will receive a list of all assets, the process on how to update the asset information, and a system for the on-going management of your assets.

INFORMATION EXPOSURE

Every day you create an enormous amount of information. You update your website, you send out press releases, you tackle problems with others via mailing lists. You publish articles and contributions to conferences. You cooperate with various universities, and students write their theses about your work. All of this is great – although not if you are inadvertently helping out someone who you do not wish to. After all, when was the last time you looked at Dropbox to see what is being shared about you and your organization?

RELEVANT APPLICATION

When you would like to determine what an attacker can find out about you, even before they attack.

OUR PROCEDURE

We will verify what is known about you and put this acquired information into context. We will connect all the dots with information from your domain name, WHOIS database, and data from social media or presentations. That way you can determine how an attacker sees you.

RESULT

A list of public information placed in the context of security. All of this from the perspective of an attacker who is doing his “homework” on you.

VULNERABILITY ASSESSMENT

We will find as many of your vulnerabilities as possible and will help you to rank countermeasures according to their seriousness and impact.

RELEVANT APPLICATION

When you already have a list of assets and you need an ordered list of issues to fix what is needed as effectively as possible.

OUR PROCEDURE

We will put your assets to the test – server, applications, operation or control systems to find all vulnerabilities possible. A list of all known vulnerabilities is without a doubt the starting point, although we won’t stop there. As we test for vulnerabilities, we will also search for vulnerabilities not publicly known, or in other words, a vulnerability which is the result of a specific configuration or customization.

RESULT

A list of vulnerabilities ranked according to seriousness as well as a countermeasure proposal.

PENETRATION TESTING

Knowing your strengths and weaknesses is important. However, discovering your weaknesses is one of the most difficult tasks. And that's precisely why we're here – searching for weak spots is what we love to do and we do it well.

We will help you to find weaknesses in your applications, infrastructure, and various processes and will then document it and propose countermeasures.

RELEVANT APPLICATION

If you have a list of your assets, a vulnerability scan implemented as well as a resolution process put in place, then it's time to determine whether it is possible to accomplish an objective like the stealing of customer data, accessing an industrial control system, or the modifying of payment information.

OUR PROCEDURE

To begin, we will establish 3-5 objectives. Testing at the network level is carried out according to NIST 800-115. For the testing of web applications, we employ the OWASP method. We will assess our findings with the help of Common Vulnerability Scoring System (CVSS).

OPTIONS

> INCIDENT RESPONSE TEST

Find out how your organization and colleagues react to an incident, or, if it is registered at all.

> EXTERNAL PENETRATION TEST

You will be informed of external risks and threats (during the test we will work outside your perimeter, simulating someone who doesn't yet have access to your network).

> INTERNAL PENETRATION TEST

You will be informed of threats and risks within your perimeter (during the test we will be inside your perimeter, simulating, for example, a disgruntled employee).

> API PENETRATION TEST

Practically every system utilizes or provides programmers with an interface. We will determine how your API reacts in this respect. Sometimes it is unnecessary to attack an application when the entire database can be downloaded with a single API query.

> WEB APPLICATION PENETRATIONT TEST

We will examine whether it's possible to circumvent access rights, acquire data which should not be publicly available or, if needed, examine another defined objective.

> PHYSICAL SECURITY PENETRATION TEST

We will check your physical barriers (fences, gates, car entrances and others), locks, the possibility of tail-gating and ways of circumventing your entrance system.

We will analyze your camera and alarm systems and the way which incidents are recorded and evaluated.

In the pursuit of collecting all relevant information, we will even go through your trash.

> The easiest way to gain access to a place is to put on a reflective vest and carry a ladder.
>
> You have calculated and evaluated risks, implemented various security systems, and have a working surveillance system.
>
> But what happens when we find out that the door to your server room is not locked?

Do you have an entrance system which uses contactless cards? We're even prepared for that. We will check whether it is possible to circumvent it, copy a card, or even to slip in completely unnoticed.

We will examine how the system deals with sensitive data, such as finger prints or palms, and whether it's possible to circumvent it and enter unauthorized. As a bonus, you will receive materials for dealing with GDPR.

And what about the camera system? Is it possible to outsmart or use as a point of entrance into your network? We will check what state it's in and whether it's possible to deactivate or if it has any blind spots.

> IOT/IIOT PENETRATION TEST

Having everything immediately at our fingertips is great. But not when it's in the hands of an attacker. We will check how your devices cope with this.

> CLOUD ENVIRONMENT PENETRATION TEST

Infrastructure such as code, cloudification, software as a service, containers, and microservices speeds up development. However, it also creates new problems. We will test everything connected to the cloud environment from access rights to freely available data to logical errors from a design context.

RESULT

Reports from penetration tests are customarily in the form of "Yes, we accomplished the specified objective," or "No, we didn't accomplish the specified objective." We will also indicate all of the findings we came across along the way.

We will not provide you with a complete list of vulnerabilities or prioritized findings – this is what the vulnerability scan is for.

We also don't like readings pages and pages of a boring document. That's why we write our reports like a non-fiction that reads as a thriller.

Of course, it will include all the things that a good report should have – an assessment, calculations, competencies, and impact factor.

Moreover, we are not merely concerned with what isn't working. So, when an attack is avoided, we will document it and give praise where due.

SOCIAL ENGINEERING

Every day there is immense amount of information coming your way. Customers are calling; you need to condense materials for a meeting; the insurance company sent a form to fill out; and on top of that, IT is calling for the second day in a row about updating the system. Any one of the above things could be a targeted attack, yet you wouldn't recognize it in the day-to-day rush.

Really though, do you know how to differentiate between a PDF with malware and an order from a customer?

RELEVANT APPLICATION

Taking a look at social engineering makes sense regardless of your security capabilities. Even if you don't have the capability to monitor outgoing network traffic nor do you have a security operations center, it's a good idea to determine how difficult it would be for an attacker to get in as well as to see how your colleagues might react. Even if you don't end up utilizing our countermeasures, at least you will be armed with the practical experience and you and your colleagues will be more alert and capable of reacting properly when you will be the target of a real attack.

OUR PROCEDURE

We will attempt to send you a fake email, we will call you, send a letter, counterfeit a CD or USB, request information from you. We will find the boundaries of where your systems and processes begin to fail. Also, we will explain the reasons why and how to deal with it. In short, everything you need to know about what works and what doesn’t.

RESULT

An overview of the scenarios we considered, which ones we chose and the ways in which we proceeded. A table is, of course, included with an overview of the number of successes and failures as well as an overall assessment.

RED TEAM

We will put together a “red team” - simulating real attackers - with the goal of improving your defense capabilities. The red team can be put together for one-time or for on-going use (we recommend the latter). The fundamental principal of the red teams is that it is not limited by scope or procedures. It goes without saying that we won’t kidnap your employees or threaten work-flow. A major advantage of on-going cooperation with the red team is that we will continuously hone our knowledge and approach; this know-how will be passed on to the blue team (defenders). The more the red team is able to perform better than an actual attacker, the more effectively the blue team will then be at protecting itself.

RELEVANT APPLICATION

Once you have the basics covered (such as maintenance of assets, management of vulnerabilities and are able to detect and react to damaging or suspicious behavior in your surroundings), then it’s time for the red team. If you are still struggling with basic measures, then we recommend that you resolve such issues before you use and develop the red team.

OUR PROCEDURE

First, we need to agree on the objectives; then we can create a realistic attack scenario and without any systems or addresses being off-limits. An attacker does not operate with such constraints, so it's in your best interest that the scenario is as realistic as possible. Next we will compile all needed information from entrance photos to long-forgotten conference files. Last but not least, we will carry out the attack by striking systems, circumventing physical security barriers, or by utilizing social engineering. We will wrap up by evaluating how the attack went and whether we achieved our objectives.

We are interested in the most believable attack simulation possible. That's why we won't be creating a script from an action film.

Surely, it's possible to snip a supplier's optical fibers and install a probe or drop a rope down into an area. We know that this is practically guaranteed to work. Yet you won't learn anything new from this.

That's why we will perform multiple scenarios and will inform you of weak objectives, so that the scenarios are appropriate in terms of time constraints and cost.

RESULT

One-time or on-going meetings with your blue team, where we will go over the findings and the ways to improve resistance and the state of your security. Moreover, we will prepare a summary and presentation for your superiors. This report will include the technical details of the procedure so the test can be repeated step-by-step. Also included in the report will be our tactical recommendations for an immediate resolution of issues as well as strategic recommendations for long-term improvements.

THREAT ASSESSMENT

We will verify whether the threat you received or detected is credible or not. Just because there is a threat, doesn't automatically mean that you have to get rid of it or invest into minimalizing it.

RELEVANT APPLICATION

When a new threat is discovered or someone declares that an attack will be carried out in the future.

OUR PROCEDURE

Our goal is to answer the question: What could go wrong? We will assess the credibility and impact of the potential threat along with the probability that the threat could realistically happen. We assess threats via the STRIDE, DREAD or ATTACK TREE methods and according to which method works best in the given situation.

RESULT

A report including an analysis and the method employed, which will clarify how we came to the conclusion that we did.

THREAT MODELING

Unlike threat assessments, threat modeling is a process of identifying all potential threats, such as structural issues, scenarios, vulnerabilities, accessible exploits, attackers, and effects.

RELEVENT APPLICATION

Threat modeling should ideally be performed during the design process and always repeated after any major changes. At the basic level, threat modeling detects, documents, and maps the relationships between attackers, vulnerabilities, attacks, countermeasures and the impacts it has on business, the organization and processes within your environment.

OUR PROCEDURE

Customarily, we begin with an attacker and a set attack scenario. Subsequently, we proceed until we detect the vulnerabilities which can be abused and the means thereof; we define countermeasures and determine how to stop them; finally, we quantify the impacts on your activities.

In addition to experts on individual security domains, our team is also comprised of a group of experts knowledgeable in the area in which you operate.

That's why our team is made up of experts in, for example, control systems, SAP, manufacturing, energy, procedural management and other areas unorthodox for security firms.

RESULT

The documentation of input parameters, assessment methods, and a description of residual risks after the implementation of certain measures. The report will include tactical and strategic recommendations in addition to the actual threat assessment.

SECURITY ARCHITECTURE

We have been with you every step of the way: from the implementing of security solutions to the designing of control systems to the implementing of security for existing systems. We have worked during operations, designed data centers and networks, and have implemented application security. All of this work has provided us with a unique perspective on problematic areas. And thanks to this knowledge, we are able to assist you in devising security architecture, from the defining of objectives to the implementing of a plan to conceiving a budget and work distribution.

RELEVANT APPLICATION

The best time for creating security architecture is the present, especially if you don't have it in place yet. And even if you already have it in place but are planning to implement new systems, applications, processes, or another change, then now is the time to re-assess your entire current security architecture.

OUR PROCEDURE

Provided you have security architecture already in place, we will revise its current state and go over requests with owners and users of assets. Additionally, we will take into account your technical and security progress from the time of the security architecture's implementation up until the present.

If security architecture has yet to be implemented, we will focus on what you would like to accomplish as an organization and what kind of progress you envision, whether technical or organizational or both. We will devise a plan on how to proceed with the development of your systems and applications, so that security does not hinder development.

RESULT

You will receive a catalog of measures which will need to be implemented as well as a diagram of relationships and principals by which to operate. All of this will take into account your operations and which systems, applications, and processes you utilize. Furthermore, the choosing of suitable technology suppliers is much easier once you have a working security architecture in place.

INCIDENT MANAGEMENT

For the resolution of security incidents, we will provide a team, instruments, and know-how. Just because you do not have a security operation center in place nor a group of operators and analysists, does not mean that you cannot properly respond to a security incident.

RELEVANT APPLICATION

This is plain and simple – the most advantageous use of incident management is precisely when you detect that something out of the ordinary is occurring and when you suspect it's an incident.

OUR PROCEDURE

We can proceed in two ways. If you have your own security operation center, we can simply fill in the blanks where your competencies are lacking (for example, application security, ICS/SCADA, or specific protocols). If you do not have your own security operation center, we can provide you with assistance during resolution of the incident, from start to finish.

At the start, we will appoint an incident leader; next, we will determine whether it's an actual incident as well as how serious it is; then, we will agree on the next steps. We will determine whether additional applications and systems were compromised or if data was leaked, and we will provide your lawyers with technical support.

RESULT

We cannot erase the incident, but we will minimalize the damage and neutralize its impact.

APPLICATION SECURITY

It's irrelevant how secure your infrastructure is or that there are protocols implemented for physical security or even that there is a detailed procedure for the management of incidents if your entire client database is downloadable with a single query to an insecure application.

RELEVANT APPLICATION

Securing an application is suitable at any stage – before initial implementation, after implementation of a new version, or even during routine operations.

OUR PROCEDURE

In order to ensure that everything is working as it should, we will use everything at our disposal – from static to dynamic analyses to fuzzing and manual testing.

RESULT

A list of our findings, a countermeasure proposal, and additional steps needed to increase the level of security.

MANIFESTO

We are fairly small for a "**boutique approach**," yet on the other hand, we are experienced enough to take on projects of any size. Moreover, from all of our years working in the business sphere, we have compiled an extensive network of developers, business and data analysts and other experts who we put to use towards the success of any given project.

We value **long-term relationships** – both with colleagues and clients; we believe that these relationships are the best indicator of our work.

We realize that time is one of our most valuable commodities. We value our own time as well as the time of others – that's why **we respect deadlines and appointments.**

Good friends stick to their agreements. That's why we'll always be honest with you, and when we have agreed to something, we will stick by it.

We are **open and honest** – you will be informed of problems politely, yet we won't sugarcoat them. This is how we communicate amongst ourselves and also how we'll communicate with you.

We don't believe that cleverness and dexterity make up for a lack of communication skills. Even if we were to come up with the most brilliant solution ever, it will not come to fruition if we are unable to properly explain it. That's why we place an emphasis on **listening and clear communication.**

We are not afraid to **admit to our mistakes**. If we make a mistake, we will fix it – but not on your watch and regardless of how much extra time it takes us. Our reputation means a lot to us.

We understand various fields, although refuse to be pigeon-holed by their limitations. During our work, we gain inspiration from many different branches, because we believe that the best things are born by bridging the divide of different disciplines.

Last but not least, with us you will **not have to be in contact with account managers or sales teams**. Simply because that's not how we operate. Each project is directly led by the person who is working on it.

ROLKEN

CONTACT & LEGAL INFORMATION

Contact details

+420 228 224 645

hello@rolken.cz

Mailing address

Rolken s.r.o.

Salmovská 1534/11

12000 Prague 2, Nové Město

Czech Republic

Invoice details

Rolken s.r.o.
Nademlejnská 600/1
198 00 Prague
Czech Republic

ID: 02155176
Tax ID: CZ0215517
DUNS: 361438111

We are registered with the Prague City Court, ref. no. C 216078.