2020-03-01

EVOLUTION SECURITY GMBH
IT-SECURITY & SERVICES

Table of Content:

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

1. Introduction

Our company protects famous software, services, applications on multiple platforms & informs the vendor in a secure way. We provide advanced penetration tests and vulnerability assessment to our customers and clients. Targeted exploitation, benefits programs, security rewards, bug bounty programs and silent or responsible disclosure is our business. Evolution Security GmbH offers its services successfully to international companies of all sizes and sectors. More than 20 corporations are still part of our customer base like many other medium-sized companies. Customer satisfaction is paramount to us, for that reason we do offer our customers in the field of safety tests to be personally on site to gain insight into our approach or workflows.

2. Evolution Security GmbH - Company (About)

Startup, Management & Founder

Founded in 2008, Evolution Security derives its authority from the world's foremost technology institution and from our moderators deep technical knowledge, creativity and unequaled access to the world's preeminent security researchers. The evolution security team exchange information in a lot of countries and work from a neutral perspective as independent security team. The independent and non-commercial security research work-sharing group has been founded in december 1997/1998. The company red-team was managed by individuals in 2008 until 2013 to handle large corporations and clients. The evolution security gmbh company has joined the it-security market with a new business model and turned in 2014 official to a GmbH. The managing director of the Evolution Security GmbH company is Benjamin Mejri (Kunz). He is also one of the company founders and the backbone in the administrators team. The company is official registered in germany (Industrie & Handelskammer) and owns an office in technology center in kassel wilhelmshöhe - Hessen.

Concepts & Services

The mythology of our company is connected to the concept generated with trust, long drafting partnerships or cooperations and of course the technical knowledge.

- Vulnerabilities, Advisories, Penetrationtests & Audits
- Protection, Prevention-Software & Cryptography
- Security-News, Discussions and commented Reports
- Programming, Researching & Security Management
- Exploitation-Videos, White+Black Papers
- Risk Analysis, Developer-Tutorials & Security Videos
- Workshops, Talks, Presentations & Trainings

Philosophy of Penetrationtests & Security Team

Our Team will work out an individual Security-Test and Penetration-Test solution for your requirements. Our Philosophy is not to test with the "usual" Scanning-Applications or scripts, we just use them as an addition to our special manual security testings. Our international Team with a long-standing expert knowledge will be glad to audit your software, online service, application and appliance solution as well as every other part of your network infrastructure.

"Our Ambition Is Your IT-Security!"

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

3. References of our Security Company

To review our external hosted press releases in partner websites or the independent press itself we prepared a great list for our customers. The listed magazines, news and press portals reported about discovered security vulnerabilities of the evolution security team in the vulnerability lab.

Reference(s): Public Security Acknowledgments

www.support.apple.com/kb/HT1318
www.paypal.com/webapps/mpp/security-tools/wall-of-fame-honorable-mention
www.adobe.com/support/security/bulletins/securityacknowledgments
www.oracle.com/technetwork/topics/security/securityfixlifecycle-086982
www.developer.att.com/developer/apiDetailPage.jsp
help.linkedin.com/app/answers/detail/a_id/37022
www-03.ibm.com/security/secure-engineering/report.html
www.nokia.com/global/security/acknowledgements/
www.us.blackberry.com/business/topics/security/incident-response-team/collaborations
www.pages.ebay.com/securitycenter/ResearchersAcknowledgement
www.technet.microsoft.com/en-us/security/cc308589
www.security.yahoo.com/article.html

4. Vulnerability Research Laboratory (About)

The new Vulnerability-Lab is now live! We are certainly excited about this project and have much to work toward. The Vulnerability-Lab works very hard in bringing Europe and the world a great amount of information regarding vulnerabilities and urgent security advisories. If you are a vendor, Vulnerability-Labs can be an extremely valuable resource for information in detail about the current state of security for your software.

Vulnerability-Lab is a research team that finds vulnerabilities, security holes, and bad security practices in software and applications, bringing this information to one site where vendors may be notified in a professional and timely manner.

The Vulnerability-Lab is comprised currently of eleven members who range from experts in the field of Information Security to managers of information and site content. All of these members, however, are greatly interested in security and is their primary concern. The research team releases, on average, 25-40 vulnerabilities a month, ranging from important to critical.

The process of releasing vulnerabilities and advisories is always generally followed in a professional manner. Sensitive Information is censored and any contribution from third parties that may include or seem to encourage malicious or stolen content, or personal/group agendas is strictly forbidden. More information are available in the main FAQ.

Not only does the Vulnerability-Lab provide advisories for software, but it also allows the customisation of these advisories down to particular vendors, types of vulnerabilities, dates, and even informative videos.

If your goal is to only be notified of security holes in your software and to work with the researchers to have it patched, then this option is naturally available. However, collaboration amongst our team and with other teams and vendors is a priority, as education and knowledge always lie in the forefront.

Read our blog or join our forum if you would simply like to read more and keep up with the fast-paced world of information security and what is going on in our labs!

Vulnerability-Lab is committed to bringing vulnerabilities to light and collaborating with researchers for the

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

betterment of software and application security.

If you are a member of a research team and would like to work with Vulnerability-Lab, send us an E-Mail including who you are and what you are interested in contributing. If you are a manufacturer or research team that would like to employ our services, we would be more than happy to oblige.

This is a very dedicated and talented team of researchers and workers. Investing in the Vulnerability Laboratory will help nurture both the security of your software as a manufacturer and also status of application and software security world-wide. Please contact us if you are interested sponsoring, benefits and internet prevention system projects for customers.

Domains: www.vulnerability-lab.com or www.vuln-lab.com

5. References of our Security Laboratory

The new category shows you as customer or client a lot of public references like advisories, own program, bulletins, press releases, pictures, competition or contest ranks and much more. The shared references are public available at external sources and some are live taken pictures are copies of the original external hosted sites.

Our team has several news sites & magazines as partners to provide exclusive security news with resources as reference. Enjoy the content and feel free to contact us or send us your feedback.

The evolution security team work with famous vendors like Microsoft, Dell, eFront, Facebook, IBM, Fortinet, FortiGuard, Woltlab, AT&T, Sonicwall, Barracuda Networks to list the security bulletins in official customer sections, resource centers, appliances, monitoring systems & other locations. The following bulletins are published by the vendor to prevent exploitation & attacks against customers or clients. We use some of the already published security bulletins as stable reference to our team.

The bulletins are published by the vendor to prevent exploitation & attacks against customers or clients. We use some of the already published security bulletins as stable reference to our team.

Link Reference(s):

technet.microsoft.com/en-us/security/bulletin/ms13-067
esupport.trendmicro.com/solution/en-US/1096805
fortiguard.com/advisory/FG-IR-013-001/
fortiguard.com/advisory/FG-IR-012-007/
fortiguard.com/advisory/forticloud-cross-site-script-persistent-web-vulnerabilities
fortiguard.com/advisory/fortimanager-and-fortianalyzer-xss-vulnerability
fortiguard.com/advisory/fortimanager-and-fortianalyzer-client-side-xss-vulnerability
fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability
fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5169
barracuda.com/support/knowledgebase/501600000013m1P
barracuda.com/support/knowledgebase/501600000013lXe
barracuda.com/kb?id=501600000013gvr
sonicwall.com/us/shared/download/Support_Bulletin_-_Scrutinizer_Vulnerabilities
sonicwall.com/us/shared/download/Support_Bulletin_SonicOS_Web_Script_Vulnerability
sonicwall.com/us/shared/download/Dell_SonicWALL_SRA_Vulnerability_Service_Bulletin
sonicwall.com/us/shared/download/Support_Bulletin_GMS_Analyzer_Vulnerability
debian.org/security/2016/dsa-3622

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6186
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0956
www.cvedetails.com/cve/CVE-2016-10999/
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7851
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2018
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6186
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6767
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3196
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8710
cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13754
cvedetails.com/cve/CVE-2017-9759/
cvedetails.com/cve/CVE-2018-20368/
cvedetails.com/cve/CVE-2018-5694/
cvedetails.com/cve/CVE-2019-13472/
cvedetails.com/cve/CVE-2019-13475/
cvedetails.com/cve/CVE-2019-13473

6. Offered Services (Pentests & Information)

The evolution security team and the vulnerability lab research team offer different kind of pentesting services to clients and customers. Feel free to watch the sub categories of the offered services and enjoy. If you have any questions regarding our services, we will answer them.

- Automated Penetration Tests
- Manual Penetration-Tests
- White Box PenTesting
- Blackbox PenTesting
- Presentations & Talks
- Live Hacking & Event Shows
- IT-Security Workshops

7.1 Manual - Penetration Tests

At evolution security, our security researchers are always one step ahead of the hackers with the latest 0day vulnerabilities. Our penetration testing team members are already well known for their manual testing methodologies and acknowledged by the most popular vendors for finding and reporting 0day vulnerabilities in major products and software appliances e.g. Sony PS3, TrendMicro Antivirus, Barracuda Network's, Paypal INC, Google, Facebook, Mozilla and many more. This gives us a unique edge while performing penetration tests for our clients.

During the manual penetration testing process, every single probe/request is carefully analyzed and monitored to ensure that we do not miss out anything. This may increase the time duration of the project however at the same time ensures 100% successful results with zero false positives.

The type of tests may vary according to the client's scope of work however listed below is a generic list of tests that our team performs during the manual penetration testing.

- Authentication
- Authorization
- Session State Management

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

- Input Validation
- Web datastores
- XML/SOAP web services
- Web application management
- Known Vulnerabilities
- Unvalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Web Session Flaws & Vulnerabilities
- Cross Site Scripting (XSS) Flaws
- Classic Buffer Overflows
- Script Code Injection Flaws
- SQL Injection Flaws
- Format Strings
- Stack- & Heap- Overflow
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

7.2 Automatic - Penetration Tests [ARPT - Automated Rapid Penetration Testing]

At times, due to specific requirements of meeting project timelines, our team uses the ARPT (Automated Rapid Penetration Testing) methodology. During this process, various tools are used. These automatic tools are developed by the skilled information security analysts and security researchers and are mostly open source tools, commercial grade toolkits and or developed in-house at Vulnerability Laboratory Research.

Since automated testing may tend to produce false positives, our penetration testing team double checks every single entry in the report manually to ensure that all highlighted bugs are valid. This improves the quality of work that we do and helps us deliver our job professionally and up to the client's satisfaction. Our team is not dependent on any specific tools and scanners. The tools used in an automated penetration test always depend on the scope of work of each project.

The type of tests may vary according to the client's scope of work however listed below is a generic list of tests that our team performs during the automatic penetration testing.

- Authentication
- Authorization
- Session State Management
- Input Validation
- Web datastores
- XML/SOAP web services
- Web application management
- Known Vulnerabilities
- Unvalidated Input
- Broken Access Control
- Broken Authentication and Session Management
- Web Session Flaws & Vulnerabilities
- Cross Site Scripting (XSS) Flaws

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

- Classic Buffer Overflows
- Script Code Injection Flaws
- SQL Injection Flaws
- Format Strings
- Stack- & Heap- Overflow
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

7.3 White Box (Whitehat) - Penetration Tests (US|UK)

Depending on the projects requirement, our team can perform complete White Box penetration testing to evaluate the efficiency of the client's network infrastructure or applications. System or network configurations, protocol specifications, source codes and the occasional password are shared with the security team prior to the tests in this approach.

This may also help to reduce the number of resources required to deliver the project. This also helps checking the system and making sure it can withstand security attacks even when some of its security information is made available to attackers or other outsiders. White Box penetration test usually requires physical access to the target infrastructure, private information or the for example application source codes.

The goal of a white box test is to check the robustness of an infrastructure or an application in its specific system environment where the security information cannot be strictly controlled. Our team works closely with your team ensuring that the flow of information and intel sharing is optimized as per clients satisfaction.

What are the advantages of the White Box security test procedure?

- Increase of number of vulnerabilities & detection rate
- Faster alignment and procedure for penetration tests & simulations
- Network Risk Analyzes for Infrastructures
- Accept new attack vectors through the developer view

7.4 Blackbox (Blackhat) - Penetration Tests

Blackbox penetration test requires no prior information about the target network or application and is actually performed keeping it as a real world hacker attack scenerio. Even though, most of the times the testing team could have access to the application source code and or the other network elements, black box testing is still preferred because it not only catches all the low hanging fruit, but also enables the security experts to look at various other levels of security including the server level vulnerabilities.

This is usually the best approach because it enables our security team to think out of the box and perform tests on all levels and according to our practical expertise and knowledge. Our security experts will use all of the tricks and methodologies at their disposal in an effort to emulate the persistence, knowledge and expertise level of potential attackers.

In this process the hacker will be only provided with the company’s website or IP address. Therefore the ethical hacker simulates all web hacking techniques (e.g. Social Engineering, Network Scanning, remote access exploitation etc.) that would be used in a real life attempt to breach security.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

What are the benefits:

- Real attack conditions
- Versatile insights & documentation
- Not disclosing your projects or source codes
-

The end goal is to verify the integrity of our client's network and applications and to proactively reduce risks that pose a direct threat from an insider / outsider hacker or other adversaries

7.5 Web Application Security

The Evolution Security GmbH security team has specialized in identifying vulnerabilities or vulnerabilities in web applications and script-based applications. Our security company is known to identify, report, and successfully close web-based vulnerabilities and vulnerabilities in applications or services. Evolution Security GmbH works closely with the various manufacturers and companies of all industries to ensure that security gaps in web applications can be identified, analyzed and successfully resolved as quickly as possible.

Among other things, during our tests, we have discovered new vulnerabilities in organizations such as the NATO, the White House, the IAEA, the NSA, the German Armed Forces, the FAA, the EU Commission, the Nasa and the Chinese Ministry of Commerce to permanently protect critical infrastructures.

Our security team examines web applications at the following levels of communication:

- Database queries and connections (MySQL, MSSQL, PostgreSQL ...)
- Client-side communication
- Server-side communication
- Application-oriented communication
- Input & Output Mechanisms

Our Advanced Persistent Threat Team identifies and analyzes the following vulnerabilities:

- Client-Side Vulnerabilities - Cross Site Scripting, Cross Site Request Forgery, Redirects, Clickjacking, SSRF, ID Hijacking ...
- Server-Side Security Gaps - Remote Code Executions, Insecure DirectObject References, Remote / Local File Inclusion, SQL Injections, Directory Traversals ...

Penetration tests are carried out according to the following scheme:

- Reconnaissance
- Enumeration
- Exploitation
- Dokumentation

Please contact us directly for inquiries, offers or orders in the area of the "Web application" & "Web Appliance" security.

7.6 Network & Infrastructure Security

Infrastructures with an information technology background are subject to a high degree of dynamism of the business processes and company requirements due to the continuous change of time. Further developments such as the virtualization of server systems or moving to the cloud require a continuous optimization of the network security components and the infrastructure to the current requirements of the

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

digital age.

Network security is a process that is to be placed in the field of secure infrastructure. This process must take place on a permanent basis in order to quickly identify permanent problems or new and known weak points.

Evolution Security GmbH accompanies, creates, defends and takes care of you in this way in the field of IT security. We create concepts for secure networks, analyze risks, assess security mechanisms, and identify known or unknown vulnerabilities.

Our team of experts can be flexibly integrated before the creation of a network, but we also gladly help with already established productive networks. We advise our customers on a reliable and secure level, taking into account all possible safety-relevant problems.

Network Interfaces & Components

Network transitions, e.g. The connection to the public Internet or ethernet network interfaces between different areas of your company must be checked, checked and regulated in order to protect the services and data from unauthorized access and ensure the network security permanently. This is the task of firewalls, filter mechanisms and intrusion prevention systems.
The Evolution Security GmbH and APT research team develops tailor-made individual solutions for your company to actively ensure network security.

Server Systems & Virtualization

The creation of server systems through virtualization constantly requires new security measures to ensure overall network security. Communication interfaces, which were previously secured by firewalls, are increasingly being outsourced to the virtualization hardware via the internal area. Existing network security solutions can't, or only adequately, provide the necessary protection.

Evolution Security GmbH supports you in aligning and adapting existing security concepts to meet the technical challenges of modern times. Please contact us directly for inquiries, analysis or assignments in the area of "Network Security".

7.7 Mobile & VoIP Penetration Tests

Smartphones are everywhere, the mobile industry explodes in 2010 to 2013 because of the endless requests to have a smart phone by apple, microsoft, nokia, samsung with different OS like Android, iOS or for example windows 8.1 preview in the pocket. Mobile security or mobile phone security has become increasingly important in the mobile computing sector. It is of particular concern as it relates to the security of personal information now stored on smartphones or mobile devices. Our experts are able to cover the following sections of the mobile cyberworld.

- Mobile Software
- Firmware
- Operating System
- Mobile Web Applications
- Hardware

The industry came up with the need for more security in the mobile/voip sector and the result was that we upgraded our local infrastructure to provide stable mobile vulnerability reports to our clients, partners and customers. In 2013 the vulnerability laboratory and evolution security research team discovered about 117

zero-day mobile apps, 15 firmware vulnerabilities and 2 hardware bugs.

We do operate in the following categories of the mobile pentest business ...

- Secure boot firmware components
- Extraction of confidential material protected by the secure enclave processor
- Execution of arbitrary code with kernel privileges
- Unauthorized access to cloud account data on mobile servers
- Access from a sandboxed process to user data outside of that sandbox
- Flaw or breach in protection mechanisms
- Access Permission, Privacy and Privileges flaws

Mobile Security Feed - Vulnerability Laboratory

http://www.vulnerability-lab.com/show.php?cat=mobile
http://www.vulnerability-lab.com/search.php?search=phone&submit=Search
http://www.vulnerability-lab.com/search.php?search=apple&submit=Search
http://www.vulnerability-lab.com/search.php?search=ios&submit=Search

Mobile Vulnerability Assessment & Reverse Engeneering
The Evolution Security GmbH can perform reverse engineering services on any app or firmware mainly regardless of the architecture. The product of this work is a writeup of the apps functionality, contents, and if requested a threat and/or vulnerability assessment of the mobile application**/**firmware**/**service.

Using our in house expertise we will perform a dual purpose security audit utilizing cutting edge automation scanners developed by Evolution-Security & Vulnerability-Labs in tandem with deep manual, line by line audits offering unparalleled coverage and security assurance to developers.

7.8 Hardware & Embed Systems - Audits & Penetration Tests

In this section of the document, we offer a hardware security service to our clients and customers. Our hardware hacking and security checks impact an audit, independent hacking methods or a strong but individual reverse engeneering analysis. We are able to identify hardware bugs and misconfigurations by manufacturers. Even hardware platins of routers, building control, smart-phones, printers and security appliances which physically located in buildings of a company, this need not necessarily belong.

Our advanced hardware hackers develop and change in creative ways technology equipment (hardware) of mostly personal but also public interest. Our team deals primarily with the hardware specific devices that contain computer equipment or computers themselves. The modification or manipulation of the analog electronic devices and electrical or mechanical equipment is our business. Insecure platin connections, electronic device manipulation, hardware misconfigurations, backdoors or other unrevealed hardware secrets will be combined with independent research, silent trust & excellent reverse engeneering analysis in order to fulfill the wishes of our customers/clients.

We are working with various programs, scripts and tools, and we are researching "how to" reverse engineer and manipulate hardware found in everyday devices like smartphones, gaming or control consoles, devices with ports and other physical stuff. Exploitation of local- & remote controls, phones or prevention is the goal of our hardware security program to overcome the physical layer.

Mostly a vendor requests to test card systems, port systems, phones and special devices with exclusive embed systems. A secret rented hall in the middle of germany provides us enough place to move and work

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

with big ATM series, embed systems of the automobile (car) industry, casino automats or hardware security projects with electronic machines (Scada) and ICS. We are prepared for big and low testings and we do our best to ensure the security of your hardware product or embed system. For sure we can not identify every bug (100%) inside of a hardware product or embed system but we scope with experience and knowledge to get excellent results.

Embed System Devices connected to Hardware

Our company does not work on protecting only the hardware components of a system, we also investigate in securing embed systems specific created to hardware. In 2013 for example a security researcher of the evolution security team discovered a vulnerability in the embed system of the sony playstation 3. Especially bugs such as the acknowledged ps3 firmware issue are in scope of our security testings, audits or checks.

Embed systems created for devices (xbox,ps3,wi,kindle) mostly require a high level innovative and creative concepts to goal successfully. Our company is able to provide innovative and creative testings with expert and advanced knowledge in embed system and device security.

Our Clients & Customers ... ?!

Casinos, Drink Water Manufacturers, Gaming Consoles with Embed Systems, Banks (ATMs & ICS), Automobile Industry (Embed Navigation Systems), Government (Billing Systems), Military(ICS), Institutions like Prisons(SCADA & ICS), Hospitals(ICS), Agencies and all kind of electronic companies or electronic equipment product manufacturers. Feel free to contact our company and enjoy the advanced research.

7.9 Automated Teller Machines

During the last year we have added a new section to our service portofolio "Automated Teller Machines Security". Our team has long term experience in the cyber security sector, especially with automated teller machines of manufacturers like Wincor Nixdorf, NCR. Keba, Hitachi, Olivetti, Diebold or GRG.

Our expertise is to discover hidden backdoors, zero-day vulnerabilities in software, service, applications and of course bugs in the design, network infrastructure, ethernet, firmware or hardware itself. Next to that our team approves the controls of privileges, domain controllers, system accounts, the boot priorities, bios setup and different other integrated modules or embed system functions. (Handelsblatt | Heise)

To demonstrate how we approve different areas that mainly affect the security of full automated teller machines, watch the listing below ...

- Bios protection (Boot Priorities, Default Configurations & Password Security)
- Examination by usage of compromising boot medias
- Efficiency testing of ids, anti-virus, firewall & protective mechanisms
- Examination of key, hdd or information encryption
- Attacks in the network (Productive systems & Test-environments)
- Security approval of operating system software
- Security approval of web-applications
- Security approval of management/service consoles (Terminal & Console)
- Security approval of interfaces (Gui, Control Panel & UI)
- Security approval of operating system core (Client & Server)
- System password checks - efficiency & weakness (BIOS, System, Network & Keys)
- Examination of the payment modules or dispenser and the hedging
- Hardware configuration check and approval for unqiue or basic backdoors (Generic Backdoors, Secret Interactions & Device Tricks or Functional Combinations)

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

- Examination of the cassette configuration approval & security mechanisms
- Scan for known vulnerabilities and security threats
- Fraud correlation system or manipulation protections approval
- Special case scenarios (Reproduce or Testing of Existing Vulnerabilities)
- Identification of Logical Bugs in functionalities (Manual interaction for manipulation)

We do offer our service to customers or companies, service providers of banks but also to the manufacturers of automated teller machines. Feel free to contact us, to arrange a meeting for preview our expertise and references. Our team is cooperating with different banks or service providers to build a strong & trusted communication network "Made in Germany".

7.10 Gamble-, Slot- or Vending -Machines Security

Our security team does not only operate with automated teller machines, we do also test your companies product series like print-, ticket- or gamble automates and interaction terminals of any kind. We do test devices for back-doors, proof for vulnerabilities in the connection, test for security issues in interfaces and firmware or identify weak points in the productive infrastructure. Through our methods, we are actively combating criminal gangs or individual criminals from Germany and abroad, who are daily on the hunt.

We are ready to go on site to check the appropriate series manually or automatically to ensure a higher level of safety. Our experts in your halls will also be glad to test equipment before the first use in order to identify safety-relevant problems at an early stage. In principle, we do not offer any blackbox security tests in this area on the basis of trust, so that we can develop reliable solutions together.

Our company helps affected companies to develop a better understanding through their own preventive measures. We offer innovative presentations on the subject for prevention for affected and non-affected companies.

Our security technicians can identify and deal with the following problems within the framework of the service.

- Vulnerabilities (Interface, System & Software)
- Weak spots (Hardware)
- Security approval of connection (Network & Communication)
- Backdoors (Secret Combinations)
- Reverse Engineering (Hardware, System & Software)

Our customers of industrial manufacturers, which we inspect with service providers for safety failures include well-known manufacturers such as

- Gauselmann
- NovoMatic (Novo Line Series)
- NSM Löwen Entertainment
- Bally Wulff

The following list shows various customers who have checked their ticket machines from us:

- Toyo Network Systems & Integration
- BSC-Europe
- Atron Electronic GmbH
- Elgeba Gerätebau GmbH
- Höft & Wessel AG

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

- ICA Traffic GmbH
- Scheidt & Bachmann
- Krauth Technologie

8. Government Program (Exchange & Cooperation)

Evolution security team cooperates with the following official universities, government academies and military institutions. We only offer this service for vulnerability research, vulnerability exchange, security trainings or workshops & security vulnerability assessment. Our new program is available to protect sensitive data, information, online services, websites, web-servers, computer systems, software and of course unofficial or non-public programs/projects.

Our team is a trusted resource for cooperation or information and we support all kind of governments (RU, CN, US,IT ,DE & Co.).

Our official Service to Government, Military, Institutions & Universities?

The evolution security team provides 3 new infrastructure services to official government related organisations, the military, universities and of course security agencies. The first of the 3 provided programs is the "Service Infrastructure" security program. The service is only available to government institutes or official organisations and impacts the testing and hardending of system specific online services. The second service of our team is the "Software Infrastructure" security program.

The software infrastructure security program allows military, government and agencies to get notified about 0day software security vulnerabilities in products of interest and the APL. The second service also impact forwarding of software core tests and audits. The third innovative service we offer to government is the "Web Application Infrastructure" security program. The web application infrastructure security program impacts the hardending, penetration testing, checks & prevention for government related online services and websites.

How to participate in the new Government Security Program?

To participate in the government security program you only need to choose one of the services (service-, software-, application -infrastructure security program) and write us a mail. There are some security regulations in our new government prevention program.

- **NO** heavy sanctioned countries like Syria, Lybia, Afghanistan, Palestina, Iraq, North Korea & Co.
- **NO** Governments or Military with criminal intentions or evil intentions for offensive operations
- **NO** Government unrelated company requests from the private or in-officials

Note: Our team does not exchange any private user contacts to governements, partner contracts, contact address of customers or sensitive company information. We also do not focus on forensics, busting hackers/crackers/fraudsters or attacking (infiltrate) other computer systems

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

8.1 SCADA & ICS Infrastructure

The scada security program is available to famous companies of the private and public industry. We share information, exchange resources and we provide excellent scada security analysis and penetration tests. The program and information exchange is connected to an available budget.

We offer a information and security service to public partners, private customers or famous clients to secure your internal or external SCADA & ICS infrastructure. Our expert penetration testers and vulnerability assessment core team is certified and trained in dealing with SCADA or ICS.

The SCADA & ICS Security Program customers and clients are drinking water manufacturers, software manufacturers, traffic management & control centers, the mobile service industry and manufacturers, food industry, electronic power grid manufacturers and much more. Feel free to join the program to get information about the new vulnerabilities in industrial control systems.

The SCADA & ICS Security Program of our (evolution-security) company does not cooperate without verification of clients, partners and customers because of security reason.

SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) **... ?!**

Is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large scale processes that can include multiple sites, and large distances. These processes include industrial, infrastructure, and facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption

8.2 Service Infrastructure Security

Our team cooperates with military institutions, government information security companies and security agencies. We provide vulnerabilities to threat systems, bug monitoring applications/systems, security appliances and of course verified security resource centers.

Zero-Day Vulnerabilities - Appliances, Security Centers & Monitoring Systems

The evolution security team provides with the vulnerability laboratory an excellent infrastructure for daily and weekly information security vulnerability news. We provide 0day vulnerabilities to security appliances, online services for monitoring or notification and of course security threat systems/centers.

As part of our program we also inform the government related contacts early about vulnerabilities to protect the own service product infrastructure and of course to heavy prevent security incidents.

Clients of our "Service Infrastructure" Exchange Partnership Program

- Vulnerability Monitoring
- Vulnerability Notification Systems

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

- National Vulnerability Databases
- IDS/IPS Vulnerability Listings
- Security Appliance Vulnerability Services
- Vulnerability Alert and Emergency Online Services

NIST, DHS, SCIP, VCW, CNNVD & Co. - Vulnerability Exchange (Service)

The top researchers of our laboratory are listed all over the world in different monitoring services or application system with discovered vulnerabilities. We are acknowledged with references in the following public government databases, DHS, NIST, VCW, CNNVD, SCIP & co.

Review the following additional pictures of published vulnerability notifications and bulletins. Feel free to contact us for exchange of vulnerability information and watch the main category with the contact information for government- institutes, security programs, institutions and the military.

8.3 Software Infrastructure Security

Our team cooperates with military institutions, government information security companies and security agencies. We provide software & product zero-day vulnerabilities to protect sensitive government infrastructures but also prevent cyber attacks.

Zero-Day Vulnerabilities - Software & Product Series

The evolution security team provides with the vulnerability laboratory an excellent infrastructure for daily and weekly information security vulnerability news. We provide 0day vulnerabilities in software for government clients to protect important internal and external software based infrastructures.

The service is especially created to exchange and share information about software vulnerabilities but also impacts a partner network software bug notification service. The program mostly focus on security and protection software products & series which are related to protect government infrastructures. We also discover vulnerabilities in software that are official listed in the yearly discovered US APL (Approved Product List) for military and government.

Clients of our "Software Infrastructure" Exchange Partnership Program

- Security Agencies
- Military
- Government Information Security Companies
- Security & Vulnerability Assessment Services

Software Security Program - Vulnerability Exchange (Service)

The top researchers of our laboratory are listed all over the world in different protection- and guard centers with discovered vulnerabilities.

Feel free to contact us for exchange of vulnerability information and watch the main category with the details for government- institutions, programs, institutes and the military.

8.4 Web Application Infrastructure Security

Our team cooperates with military institutions, government information security companies and security agencies. We provide 0day web application vulnerabilities and excellent security tests to protect government infrastructures. We are well known for detecting 0day web vulnerabilities in all kind of online service infrastructures like banks, airports, government websites and service or military networks.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

Researchers of the evolution security team have already discovered 0day vulnerabilities in the web application infrastructure of the nato, the whitehouse, the iaea, the nsa, the nasa or the chinese ministery of commerce and much more.

Zero-Day Web Application Vulnerabilities - Online & Web Services

The Evolution Security Company and the research team provides an own web application infrastructure security programm for Government- or Military institutions.
In the first place we provide the service only to verified and trusty clients, to audit, penetrate or do any other related security check.

The seconds service in this area is the vulnerability laboratory, which tracks vulnerabilities actively to secure critcal government infrastructures.

Clients of our "Web Application Infrastructure" Exchange Partnership Program

- Government Banking & Transaction Applications
- Government Service IPS Application
- Government, Army & Military Website Applications
- Military Web Applications & Control/Management Interfaces
- Government Online Service & UI (User Interfaces)
- Web Filter-, Secure Engine and Protection Web Applications

Application Security Program - Vulnerability Exchange (Web Applications)

We detect all kind of session problems, encoding flaws, cross site issues, filter & secure engine bugs, sql injections, auth bypass vulnerabilities & more.

Feel free to contact us for exchange of vulnerability information & watch the main category with the details for government- institutions, security programs, institutes and the military.

9.1 Reconnaissance (Information Gaterhing)

Technical - Reconnaissance

Technical information could be for example sensitive errors, web-server hosting/information, ips/ip-ranges, knowledge about hardware or software versions, modules or models, information about the internal or external network infrastructure of a company.

Non-Technical - Reconnaissance

Non-technical information could be for example internal company structures (office), location (company) and area (country) information, employee, internal phone numbers, email addresses to social company contacts.

Non-technical information are mostly bound to the social and structure of the target company.

Combining the Technical & Non-Technical

Both part of the information gathering sector can be combined on each test case in a separate way to grant excellent penetration testing results. Sometimes a company has an internal non-technical structure problem. Remote attackers can combine the non-technical with a technical information to successful perform an attack against the target company. We combine the non-technical with the technical information gaterhing procedure to secure infrastructures.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

Public Information - Only!

All the data and information we capture or gather are accessed without vulnerabilities or exploits. During the reconnaissance phase no active cyber attacks or actions are taking place, the company computer systems are completely safe.

Next Phase Exploitation

After the information gathering process in the reconnaissance phase, the next step would be the enumeration phase. Watch the enumeration phase information as next step.

9.2 Enumeration (Attack Vectors)

The enumeration phase is the phase where the information of the reconnaissance phase will be in use the first time. The enumeration procedure impacts for example active actions taken by cyber attackers to gain system access and of course the important attack vectors or schemes. Information and Data captured through the reconnaissance phase build an review and overview about the target company. In special later test cases or topics the captured information plays a significant role in the enumeration or exploitation phase.

During enumeration phase, date and information will be systematically captured or tracked. In special cases individual systems, infrastructures or environments are complete identified by our security team during the enumeration phase simulation.

Enumeration ... ?!

An enumeration of a collection of items is a complete, ordered listing of all of the items in that collection. The term is commonly used in mathematics and theoretical computer science to refer to a listing of all of the elements of a set. In statistics the term categorical variable is used rather than enumeration.

The precise requirements for an enumeration (for example, whether the set must be finite, or whether the list is allowed to contain repetitions) depend on the branch of mathematics and the context in which one is working. Some sets can be enumerated by means of a natural ordering (such as 1, 2, 3, 4, ... for the set of positive integers), but in other cases it may be necessary to impose a (perhaps arbitrary) ordering.

In some contexts, such as enumerative combinatorics, the term enumeration is used more in the sense of counting – with emphasis on determination of the number of elements that a set contains, rather than the production of an explicit listing of those elements.

Next Phase Exploitation

After the reconnaissance and the enumeration -phase, we are prepared for the exploitation phase. Watch as next step the exploitation phase information.

9.3 Exploitation

The exploitation phase is the third step of the test simulation procedure. In the exploitation phase the researchers and pentesters take action by actively exploitation of security flaws, well know vulnerabilities, zero-day vulnerabilities and security weaknesses. Our top researchers combine to manual and automatic exploitation methods to successful goal.

Development - Exploits & Proof of Concepts

In the exploitation phase our security researchers and penetration testers develop own exploits to bypass or

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

evade filters but also to unauthorized gain system access by own discovered zero-day vulnerabilities. Once our researchers against unauthorized system access to a first or main system the possibility popups up to continue the exploitation procedure with the followup target systems.

In the exploitation phase our researchers attack the computer systems with high experience and of course our own software, scripts or programs.

Public Bugs - Exploits & Proof of Concepts

We are also able to use public vulnerability reports, poc and exploits to successful detect vulnerabilities in customer infrastructures but our main priority on testings is to discover zero-day (unknown) vulnerabilities. The evolution security team is also watching and monitoring public information about public vulnerabilities or bugs to grant our clients/customers an all around exploitation simulation.

Re-enter of Reconnaissance & Enumeration

In the exploitation phase the researchers and penetration testers have ever the ability to re-enter the reconnaissance or enumeration phase to capture new targets and also to extend running tests.

Next Phase - Documentation

After the exploitation -phase, we are prepared for the documentation and ending phase of the simulation. Watch as next step the documentation phase.

9.4 Documentation

The clean documentation ensures that the issues can be reproduced or reconstructed for analysis by the vendor or developer teams. The documentation will be written by the researchers and penetration testers who performed the penetration tests or security audits. The documentation will cover all penetration test results with innovative information as highlight and productive security details. We ensure that the documentation perfect covers the penetration tests with all important details concerning the individual findings.

Detailed Penetration Testing Reports

Our reports are splitted to several informative parts. At the beginning, there is a introduction and summery. The summery and introduction provide details about the vendor, servers and of course the software or product itself.

The second part impact the technical details of the open security issues detected in the customers computer systems.

The third part impact the exploitation information of the bug or vulnerability with a detailed proof of concept and in special cases also manual exploitation steps for reproduces.

The last part of a documentation snippet impact for example a solution to patch the security bug and of course a risk analysis by the security researcher or penetration tester. Mostly the reports will be attached together with all resources to produce a final documentation in the last phase.

After the last Phase ... ?

After the last phase the evolution security team is ever responsible for security questions, problems, assistance to reproduce and of course a future cooperation. Become a partner of our strong security network and stay secure with permanent checks, tests, reports and analysis by the evolution security core team.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

Corporate Security Report (Individual Areas & Entire Company)

Evolution Security GmbH offers you uniform corporate security reports that are specific to individual infrastructure areas, such as: build the data center. In addition, our company offers a complete assessment of your entire digital enterprise infrastructure. The complete assessments include topics such as physical security, infrastructure stability and integrity checks, access security and monitoring & monitoring. Further details on the subject can be found in our service documents.

Management Summary (Works Council, Management, Investors & Customers)

Do you need the safety documentation as a summary for different departments of your company? This is not a problem either, we offer tailor-made management summaries in the security documentation, no matter which department it is due for. Whether for the works council, the management or investors & customers, the Evolution Security GmbH manufactures a transparent and tailored to the department document in order not to confront potential employees with unnecessary, incomprehensible details

10. Events & Conferences

10.1 IT Security Presentations, Lectures & Talks

Evolution Security provides stable commercial talks which are getting extended in a period of every quarter per year to make them unique and perfect.

The talks are very informative for researchers, security companies or penetration tester to learn about manual way of exploitation, basic and advanced protection, bypass methods or secure programming.

Our company does not only offers workshops and presentations, it does as well live shows for hacking events and conferences. As in other subject areas, the emphasis here is on IT security.

Security Talks, Presentations & Workshops

To get an overview on the various training courses, workshops and to give live shows, we have extra hacking compiled for you the following information. All our training courses, lectures and performances require no previous IT knowledge.

Only if a workshop or a presentation with advanced or expert is instantly highlighted in the title, we require a technical knowledge for your understanding. The training courses and workshops take an average of 1-2 day (s) to complete and include short breaks.

The live shows of Hacking take between 30-60 minutes and 60-120 minutes between our presentations, those are ideal for conferences or training sessions.

Excellent Speaker & fresh Topics

We provide excellent & exclusive workshops around topics like phone/mobile security, zero-day software & application bugs, firewall & filter pentests. Check them out and book 1 or 2 sessions for your company, event or prv8 team.

The evolution security team researchers also participate as speaker in security conference after invitations or special request. Enjoy the live workshops, talks or presentations by our official & well known company experts.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

10.2 IT Security Workshops

The Evolution Security Research team offers various kinds of IT security workshops and awareness workshops, combined with a training, many technical details, a bug analysis, code review, sample codes, source texts, images and exclusive expertise.

Especially the awareness training courses are of great importance for fresh employees or company foundations. Today, employees are exposed to many security risks that result in an unsafe infrastructure. This problem is highlighted in several of our workshops / awareness-trainings & contains special recognition features in dealing with electronic media & sources.

Note: Every month the workshop listing gets updates because of the internal company capacity.
https://www.evolution-sec.com/en/products/it-security-workshops

10.3 Live Hacking & Event Shows

At evolution security, our researchers are constantly involved in 0day vulnerability research and new exploitation vectors.

Our team of security experts is well equipped with multiple years of practical industry knowledge and their published research is already accepted by major vendors across the world. This gives us an opportunity to share our expertise and knowledge with our clients.

We have designed special live hacking events where we demonstrate the most advanced methods of 0day exploitation.

This enables our clients to fully understand how different cyber attack vectors or schemes work and how they can protect their infrastructure and web applications against the most sophisticated cyber attacks of today.

Some of the topics covered are:

- Zero-day Filer Evasion & Filter Bypass (Advanced evasion techniques)
- Zero-day Vulnerability Research
- Advanced Rapid Penetration Testing
- Zero-day Kernel level exploitation
- Advanced Malware Reverse Engineering

Since our team is not dependent on any proprietary tools and exploits, most techniques demonstrated during our Live Hacking Events are 0day and based on manual methodologies discovered by our own researchers. We cover everything, starting from network and system level exploitation to web application level bugs and vulnerabilities. You can contact us for more information regarding our Training and Live hacking Events programs.

11. Vulnerability Disclosure Policy

We verify the vulnerabilities & send the complete advisory to the product vendor. After the notification & the patch work-around we publish the advisory as a stable reference with author credits. We also request CVE-IDs & try to publish our information to different sources like news-sites, agencies, institutions, security monitoring services, magazines, rss feeds or mobile blogs.

Our clients and customer can choose the right way of disclosure by there own because we provide three flexible standard modules. Silent Disclosure, Responsible Disclosure & Full Disclosure.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland

11.1 Silent (Non-Public) Disclosure

The silent disclosure model of our company is new & uses the regular vulnerability disclosure policy but impact also some important changes in the phase ending procedure. The vulnerabilities in the silent disclosure program will not be public visible after a patch has been disclosed by the manufacturers company or product vendor.

In the silent disclosure program the researchers will sign a special contract with impact of a non-flexible confidentiality or secrecy document. After the reward or patch the researchers are not allowed to talk about the security incident. The public disclosure of the bug and the resources is not allowed because of the silent disclosure policy.

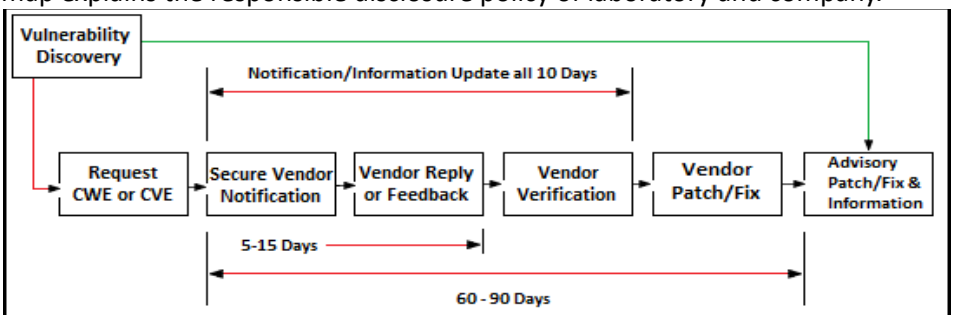
11.2 Full Disclosure

The full disclosure model of our company is free to choose. Sometimes vendor or manufacturers see a reason to directly disclose information of zero-day vulnerabilities and bugs. The full disclosure model allows the researcher or author to directly disclose his bug find after passing the internal validation procedure of the laboratory or evolution-security.

List of Full Disclosure Bugs: (Example)
Vulnerability Laboratory - Independent Vulnerability Database (EU)
PacketStorm Security - Vulnerability Database (UK)
Offensive Security - Full Disclosure Exploit Database (US)
SCIP CH AG - Bulletin Notification System (EU)

11.3 Responsible Disclosure

The following map explains the responsible disclosure policy of laboratory and company.



12 Contact & Social Networks

Our company owns several social network accounts in facebook, flickr, google+, twitter or youtube. Be welcome to visit our services ...

- https://twitter.com/Evolution_Sec & https://www.facebook.com/SecEvolution

13 Partners & Cooperations

Contact us for a stable & trusted partnership or commercials! We provide a free banner exchange website for active security projects, services, bugbounty programs, official & legal websites or labs. The evolution security company and vulnerability laboratory is watching for long period partnerships with manufacturers, clients, customers and companies to optimize.

Firma: Evolution Security GmbH
Adresse: Ludwig-Erhard Straße 4
Geschäftsführer: Benjamin Mejri (Kunz)
34131 Kassel
Telefon: +49(0)561-40085396
Land: Hessen - Deutschland