Microsoft Active Directory Security Assessment

Security analysis and recommendations to strengthen your Microsoft Active Directory

Attacks on companies and public institutions are steadily increasing. The main goal of such attacks is either blackmail and / or gaining access to sensitive information. Both present enormous risks as they can cause immense harm and sometimes cause massive financial damage.

One of the main targets is your Active Directory deployment as whoever gains control of your AD (and that's easier than most people think) gains full control over your environment.

Why is getting control over your AD not that hard? Because deployment, migration, configuration, or operation of Microsoft Active Directory is not that simple due to the many configuration options and its complexity. And this very often leads to misconfigurations that are causing vulnerabilities.

FAST LANE
Central Eastern Europe

T +386 1 320 78 80
E info-cee@fastlane.net
W fastlane-cee.net

Gold
Microsoft Partner
Microsoft

Why Active Directory security assessments?

- Prevent criminal attacks on your IT systems
- Protect your digital assets like systems and data
- Identify and fix vulnerabilities
- Minimize the risk of information leakage and expensive blackmail claims
- Comply with regulations that apply to your company
- Maintain your good reputation.
- Protect customers, partners and third parties

What's included in the assessment?

The Active Directory security assessment is carried out in two stages by our experienced and highly certified security experts.

After the initial analysis you will receive recommendations for specific measures that enable you to independently eliminate identified weak points. Once you have implemented the recommended measures, a second analysis* will show the effect of hardening the Active Directory and any remaining vulnerabilities. Wrapping it up, final documentation, evaluation and recommendation for action are handed over and will be jointly discussed.

* *The second analysis is an optional service and can be consumed within six months of the completion of the first analysis. There are no additional costs involved.*

Approach

At the beginning of the security assessment, all necessary information is collected in cooperation with the project participants and a course of action will be discussed and agreed.

Then, we will provide you with a number of analysis tools that need to be executed by you on a member server and the results need to be transferred to us. Please note that the exchange of data will always be performed secure, encrypted, and GDRP compliant via DRACOON.

Our security experts will analyze and evaluate the data and will provide you with comprehensive documentation of the results and our recommendations for eliminating identified vulnerabilities. After that, you should use this catalog of measures to harden your system. Once this has been done, you may request a further test including a corresponding analysis and evaluation.

Using the results of the second test we will perform a final review where we will discuss the results and compare them with the results of the first test. If necessary, we will recommend further measures to harden the Active Directory.

Security Assessment and corresponding recommendations

01 Kickoff-Call (remote)
02 Execution of the Analysis Tool
03 Examination and analysis of the results by our Security Experts
04 Presentation of the results and our recommendations
05 Implementation of the recommendations by the customer

Optional: Second Analysis and final recommendations

06 Second execution of the Analysis Tool
07 Examination of the results, comparing them with the previous results
08 Final call with the customer, discussion of the results and implemented suggestions

Services & Responsibilities

Fast Lane Services	Customer Responsibilities
Kick-Off Call (remote)	
• Generic introduction and overview • Collecting all relevant information • Verifying customer-related requirements • Defining contacts and schedule	• Ensuring the attendance of technically responsible employees • Providing all required information related to the corresponding active directory
Executing the Analysis Tools (initial test)	

• Providing selected analysis tools (3-5, depending on your infrastructure)
• Collection of results
	• Decompression and execution of tools on a member server via CMD, no installation required
	• Minimum server requirements
	  ◦ 4 Gb RAM
	  ◦ 2 CPUs
	  ◦ Domain Joined
	  ◦ One logged in domain administrator
	• Packing and forwarding the results (e.g., ZIP file)

Examination and Analysis of the Results	

• Examination, analysis, and documentation of test results
• Providing comprehensive documentation
  ◦ Explanation of findings
  ◦ Recommendations for fixing all detected vulnerabilities
	• None

Presentation of findings and recommendations (remote)	
• Comprehensive presentation of findings and recommendations • Responding to any questions regarding our recommendations • Discussion about second test after recommendations have been implemented	• Ensuring all stakeholders are in attendance • Preparing for the call by reviewing our documentation prior to the call • Asking questions related to our findings and recommendations
Implementation of recommended measures	
• If requested, we are happy to help with the implementation of our recommendations, but this requires a dedicated order and statement of work as this is not included in this package	• Implementation of recommendations

Fast Lane Services	Customer Responsibilities
Executing the Analysis Tool (second test)	

• Providing selected analysis tools (3-5, depending on your infrastructure)
• Collection of results
	• Decompression and execution of tools on a member server via CMD, no installation required
	• Minimum server requirements
	  ◦ 4 Gb RAM
	  ◦ 2 CPUs
	  ◦ Domain Joined
	  ◦ One logged in domain administrator
	• Packing and forwarding the results (e.g., ZIP file)

Examination and analysis of the results of the second test	

• Examination, analysis, and documentation of test results including comparison with the results of the first test
• Providing the final documentation
  ◦ Explanation of all findings of the second test
  ◦ Additional recommendations (if required)
  ◦ Final evaluation of implemented measures
	• None

Final presentation and discussion	
• Comprehensive presentation of findings (both tests) • Discussion and evaluation of both tests and implemented recommendations • Responding to any questions regarding additional recommendations	• Ensuring all stakeholders are in attendance • Preparing for the call by reviewing all provided documentation prior to the call • Asking questions related to our findings and recommendations

Pricing

We offer this Active Directory Security Assessment for a fixed price of only € 3,990 (plus tax, if applicable).

Please note that invoicing takes place after step four and that this price is true for a single domain. If a number of domains need to be analyzed then we will charge one analysis per domain.

Contact us

If you need further information, please contact one of our sales representatives or contact us via **www.fastlane-cee.net/contact**

Gold Microsoft Partner
Microsoft