Security Measures in MRPeasy

Contents

Introduction

Security is of paramount importance to MRPeasy. We put in place a comprehensive set of organizational and technical measures to ensure security of your data. In addition, there are things you can do to make sure your data is well protected.

If you currently keep your data on your own servers, the odds are that we offer a better level of security than what you currently have in place.

What do we do to keep your data safe?

General hosting and data security rules

1. We have appropriate technical and organizational measures in place to provide our service in accordance with industry and government regulations.
2. All our operations are performed solely by authorized staff following documented instructions.
3. MRPeasy software and databases are located on dedicated physical servers. We do not use virtual servers where the same physical hardware could be used by someone else.
4. Access to servers and data is limited to a small number of authorized personnel.
5. Our customers do not have direct access to the MRPeasy servers. They can access them only via the MRPeasy application user interface.
6. We wipe out all data from storage devices before utilizing them.

7. We perform the necessary system, software, and hardware maintenance on a regular basis.

Service backups and disaster recovery

8. We continually make data backups and regularly copy them to a separate location.
9. In case of fire or another disaster at the primary data center, your data will not be lost.
10. Backups are encrypted.

Connection

11. Internet connection between your computer and the application server is encrypted using industry standard SSL/TLS 1.2 technology.

    You can safely use our software when connected to public wireless networks because if someone tries to scan the network signal, your data will not be readable.

Customer data

12. Authorized MRPeasy personnel may access customer data only as required to provide the services, to prevent or resolve technical problems and customer support issues, or upon customer request.
13. By default, MRPeasy customer support staff does not have access to customer's data. If access is required to resolve a support request, it must be explicitly granted by the customer.
14. Customers can create a backup of their database and restore it at any time.

15. Customer database backup can be restored only by the same account that created the backup. A backup is valid for 30 days.
16. All MRPeasy support and technical staff have signed strict confidentiality agreements .

Additional security measures

17. Customer support requests are handled via the ticketing system which is a part of MRPeasy service. This ensures secure communication.
18. Customers are required to use strong passwords.
19. Users are automatically logged out after a 30-minute period of inactivity.
20. We provide the option to limit the IP addresses from which the MRP service can be accessed.
21. We provide the option to use two-factor authentication for login.

Hardware failure recovery process

22. Comprehensive 24/7 automatic monitoring ensures that support personnel are notified not only in the event a server becomes unavailable, but much earlier, when there is a risk of malfunction.
23. We always keep secondary servers running as hot spares. If the primary server fails, the system will automatically fail over to the hot spare.
24. Our typical monthly service uptime is 99,9%. The 0,1% of unavailability is set aside for planned maintenance on weekends one or two times per month, not for any unplanned service interruptions.

Security auditing

25. MRPeasy service is routinely audited by a 3rd party cyber security firm.

Cyberattacks

26. MRPeasy has measures in place to mitigate cyberattacks against the service. See the section “DDoS mitigation” at the end of this document.

What can you do to keep your data safe?

1. ### Be sure to keep your password private and secure.

   Be aware of phishing scams, and do not ever enter the password on any site other than MRPeasy; use a unique password with MRPeasy; update your password regularly.

2. ### Restrict user access permissions on a need-to-have basis.

   You can customize each user’s access permissions in Settings -> Human resources.

3. ### If your company has a static IP address, restrict access to your account only from this IP address.

   You can configure allowed IP addresses in Settings -> System settings -> Allowed IP. See the following documentation link for additional details:

https://www.MRPeasy.com/documentation/settings/system/allowed-ips

4. Use two-factor authentication.

This feature is available if you have an Enterprise package. It can be enabled in Settings -> System settings -> Enterprise functions. See the following documentation link for additional details: https://www.MRPeasy.com/documentation/settings/system/enterprise-functions/two- factor-authentication

5. Log out of MRPeasy when you leave your computer.

6. Keep regular backups of your database.

You can create a database backup in Settings -> Database maintenance. . This will allow you to restore the data in case of an accidental or unintentional deletion or modification.

7. Contact us via the ticketing system for secure communications.

Support tickets can be submitted at Settings -> Support.

8. Keep your contact records up to date.

Notify us promptly in case of changes.

DDoS mitigation

In a DDoS (distributed denial-of-service) attack, an attacker intentionally sends thousands of fake requests to overload the system. As a result, valid requests can only be processed very slowly or not at all. A massive number of compromised computers (a botnet) is used to create a gigantic amount of data traffic. A successful DDoS attack can cause significant downtime for web applications.

The security solution: DDoS protection

Our datacenter has implemented DDoS mitigation tools based on sophisticated hardware from leading vendors Arbor and Juniper . This three-layer system enables us to clearly distinguish between valid traffic and malicious attacks.

1. Automated recognition of attack patterns

In addition to recognizing an attack based on the amount of network traffic or the number of packets, Hetzner is able to automatically identify the type of attack and react to it. For example, a UDP flood with 500k pps is harmless for a server. A 500k SYN packet, however, could pose a problem. The DDoS protection tools can detect this type of difference.

2. Filtering traffic for known attack patterns

This method allows the system to effectively filter out the most common attacks by putting incoming requests through traffic scrubbing filters. It is especially effective at scrubbing out the following types of attacks: DNS reflection, NTP reflection, and UDP floods on port 80.

3. Challenge-response authentication and dynamic traffic filtering
In this final layer, attacks in the form of SYN floods, DNS floods, and invalid packets are filtered out. In addition, it can adapt to other unique attacks and reliably mitigates them.

Collectively, these technologies support a high level of protection, which is continually optimized. The system is improved by analyzing each attack and adjusting filters and responses.

How it affects customers

The system can detect DDoS attacks in real time, and its ability to recognize them continually improves. Once an attack is recognized, the dynamic DDoS protection tools filter it out immediately, thereby preventing system overload. Legitimate network traffic is not affected by the DDoS protection system.