RISCO

A LIFETIME OF SECURITY

RISCO Cloud Security

Introduction

As a pioneer in cloud-based Security and Intrusion solutions, RISCO fully understands the security implications of the cloud model. Based on the Microsoft Azure Cloud platform (amongst other solutions), our cloud platform is designed to deliver a higher level of security than many traditional on-premises solutions. RISCO uses its own cloud-based services to control and access our own security and intrusion systems, on the same platform we make available to our customers. That is why security, data protection, and of course privacy are major contributing factors in the design process of our solutions.

Security is central to our everyday operations, in many aspects - from designing our hardware and software solutions, selecting suitable personnel, conducting audits, and performing constant reviews.

This whitepaper outlines RISCO's approach to the RISCO Cloud security platform and focuses on the details of organizational, technical and procedural controls of security and data protection at RISCO.

The Right Personnel

Background Checks

As part of the hiring process, RISCO performs thorough background checks on each of our future employees, with emphasis on future employees in the Cloud domain with access to the Cloud. RISCO verifies the employee's employment history, education certifications, and conducts a security interview for each employee with our in-house Chief Security Officer (CSO).

Internal Specialists

RISCO has a dedicated internal architecture and security team that complies with security requirements and the latest standards. The team determines the controls, processes, and systems needed to meet these standards. In addition, the team facilitates and supports independent audits and assessments by third parties.

Active protection

The RISCO Cloud platform runs on a Microsoft Azure platform, which ensures a high level of security, data protection, and data privacy.

Additional information on Microsoft Azure security and data privacy is available at the following link:

http://download.microsoft.com/download/1/6/0/160216AA-8445-480B-B60F-5C8EC8067FCA/WindowsAzure-SecurityPrivacyCompliance.pdf

Vulnerability Management

RISCO administrates a vulnerability management process that actively scans for security threats by means of commercially dedicated tools, intensive automated and manual penetration attempts, quality assurance processes, software security reviews and external audits. Our dedicated security team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The team tracks these types of issues and follows up frequently until they have verified that the issues have been remediated.

Monitoring

RISCO's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as, the presence of traffic that may indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. Network analysis is supplemented by examining system logs to identify unusual behavior, such, as attempted unauthorized access of customer data. RISCO's Technical Assistance Center team also actively reviews inbound security reports and monitors the network traffic and status.

Security measures

Layer Separation

RISCO's Cloud platform is designed so that the different server roles are separated into virtual networks (VNETs).

Among other things, VNET are used to provide the RISCO Cloud platform with extra security, cut down on unwanted or unnecessary traffic, reduce broadcasts, ease network management, and as a result, minimize the chance of a potential breach in one layer to affect another layer.

Network Encryption

All of RISCO's Cloud platform network connections, from and to RISCO's Apps, Web interfaces and devices, are encrypted using the latest encryption standards and methods, namely SSL (Secure Sockets Layer) which supports version SSL 3.0.

All connections from and to the Cloud platform require token based authentication, or a signed certificate (where applicable) preventing any unauthorized access to the platform.

Firewall (FW)

RISCO's Cloud platform uses Azure services to defend against various attack attempts, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

Web Application Firewall (WAF)

RISCO's Cloud platform also uses Azure's WAF, among other solutions, to protect the Cloud platform services against various attempts of code and SQL injection, by providing URL filtering abilities and much more.

Periodic Assessments

RISCO conducts multiple assessments of the Cloud's security, including risk assessments and penetration tests that are performed by independent 3rd parties and managed by RISCO's dedicated security team.

Risk Assessments

RISCO well understands that an exploitation of a vulnerability in our solution could lead to a compromise of our customer's information and assets they are trying to protect.

That is why as part of RISCO's risk management program, RISCO, from time to time, performs risk assessments of its Cloud platform services and infrastructure to detect and prevent any exploitation of a possible vulnerability.

The risk assessment is performed by a 3rd party cyber Security expert company, which has developed a systematic approach, modelled on best practice methodologies and frameworks, including OWASP, ISO-27001, OSSTM and NIST for conducting security reviews and risk assessments.

Once a vulnerability requiring remediation has been identified and reported to RISCO, it is logged, prioritized according to severity, and assigned an owner. The Security team tracks such issues and follows up on them frequently until they can verify that the issues have been remediated.

Penetration Tests

RISCO conducts periodic penetration tests of our Cloud platform's interfaces, performed by one of the leading companies in the field of Cyber & Information security in Israel.

The tests performed include Black Box Penetration tests on RISCO's systems, which include some elements of Gray Box tests. Detailed reports are delivered to RISCO's dedicated Security team, and are prioritized according to the severity of each vulnerability.

Once a vulnerability is identified and reported to RISCO, it is assigned an owner according to its severity. The Security team tracks such issues and follows up on them frequently until they can verify that the issues have been remediated.

24/7 Availability

The RISCO Cloud platform runs on a Microsoft Azure platform, which ensures, among other things, full redundancy results with high availability (more than 99% up-time).

Low Latency and Highly Available Solution

RISCO designs its platform to be highly redundant. This redundancy applies to our server design, how we store data, to network and Internet connectivity, and to the software services themselves. RISCO's solution is not dependent on a single server, or network connection. Our solution is deployed on multiple data centers that are geographically distributed. The Cloud platform is intended to handle a huge amount of connections and data. In the event of any kind of failure, all platform services are automatically shifted from one data center to another, to enable uninterrupted availability, and protect users from any data loss.

Scaling Out

RISCO's platform supports rapid scale out, supporting a continuous increase in the amount of data and number of concurrent users and connections. In case the system detects a certain load in a specific service, we simply add another service in a matter of minutes.

Data Backup

The Cloud platform uses multiple Database and Storage solutions, supporting high availability and redundancy. All storage and data are automatically synced and backed up across multiple data centers, allowing the Cloud platform to recover from any failure or disaster without any data loss. This ensures continuity and high availability of our services.

Conclusion

The protection of our users' data and our system's stability and availability are primary design considerations for all of RISCO's infrastructure, products and personnel operations.

We believe that by using the Microsoft Azure platform, as well as other 3rd party platforms together with our own in-house solutions, we can offer a level of protection that very few solution providers can match. We make big investments in security, resources and expertise that free you to focus on your business. Data protection is more than just security. RISCO is committed to protect your data and provide a secured and stable platform.

For all these reasons and more, RISCO is one of the leading Security and Intrusion solution providers in the world. RISCO will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner.