Let's go further

SECURITY IN EG

Security in EG

Contents

Organization of cyber and information security

In EG we constantly seek to improve our security setup to ensure that a high level of security is maintained. We introduced an enterprise-wide cyber and information security program governed by security committees and implemented by our central security team in close collaboration with business units.

The overall responsibility for cyber and information security at EG lies with the security committee (EG Cyber & Information Security Committee) which focuses on strategic alignment of security with organization's goals and makes key decisions related to the implementation of security strategy, initiatives, controls and risks. EG's security committee, where corporate management is represented, overlooks operational performance, as well as prioritizes the security initiatives and ensures alignment with the business operations.

The security committee is represented by employees from top management, including: CEO, CFO, division EVPs, CTO, CISO and the Head of Group Legal & Compliance. The security committee reports directly to the Executive Board of EG. The committee is normative and based on the adopted security policy, it lays down the principles, priorities and guidelines that are to ensure that objectives are met. Security incidents, security status, progress on key initiatives, risks and security weaknesses are reported to the security committee. Members of the security committee regularly participate in relevant security awareness training.

Central security team (EG Information & Cyber Security) delivers central security capabilities, services, and technologies for the other parts of the organization. Security team develops and applies common security standards across the organization. Central team cooperates on the different security related activities performed on the business units' level with the appointed local security coordinators. Security incident managers are appointed in every business unit to coordinate response activities in case of a security incident.

EG adopted industry leading Center for Internet Security (CIS) Controls security framework to manage security program, measure current maturity level, define target state, and introduce common security mechanisms across the organization. We also extend our security management into areas resulting from ISO 27001. The security level in form of compliance with CIS controls is measured regularly for all products. Also the plans to improve security standing and CIS compliance are formulated and documented. The security level and progress on improvements is constantly monitored (through at least monthly reviews) and reported to management in form of dashboards. This is performed together with (and is an element of) risk management and monitoring – please see further description in risk management section below.

The security is executed through internal strategy, policies, standards, procedures, and guidelines. Every employee in EG is responsible for operating in accordance with established security guidelines during the daily business activities. The employees' direct manager is responsible for monitoring that the employee complies with group related policies and procedures that support the security policy as well as with local guidelines and procedures.

Security Risk Management and Security Level Monitoring

Management of information and cyber security is based on risk. In EG, we perform the constant monitoring of risk and security levels, as well periodical (annual) risk assessments for all products. All risk management activities are performed for all layers – application, infrastructure, network and processes.

Risk identification. Our risk assessment and monitoring process is based primarily on compliance of particular products, systems and processes with CIS Controls. CIS control coverage and maturity is constantly assessed and monitored in order to derive the residual risk level and create action plans. Additionally, risks are identified continuously - and subsequently evaluated - through other security monitoring and assessments techniques, such as vulnerability scans, application scans, pen tests as well as audits and risk assessments.

Risk assessment. All risks identified through any of the activities above, are instantly assessed and overall risk classification for products is reevaluated to reflect the risk. Risk management is performed with consideration to risk probability and impact. All risk assessments and risk monitoring activities take into account the impact of potential risk on EG, but also on our clients as well as physical persons (in case of personal data processing) – which fulfills the requirements of GDPR and NIS2 regulations.

Risk treatment. For all risks, risk treatment plans are formulated (in particular remediation actions).

Monitoring of risk, risk treatment and security level. All risks, together with progress of their remediation, are registered and reflected also in form of product dashboards, providing near real-time visibility into risks for the management - for each product, documentation of risk level, CIS scores and open risks is maintained in form of dashboards. All risks and remediation actions are monitored constantly through a framework of security meetings, reviews and committees, which ensure that risks receive the attention of management of appropriate levels – depending on the risk assessment risks are reported to Divisional or highest EG level).

Documentation. Risk management is documented in form of policies and procedures. Risk register is maintained (including remediation plans). Additionally risk rating of all EG products is maintained, reflecting the risk identified and assigned to particular products.

Security Strategy

EG developed and maintains a formal security strategy. It is documented and regularly reviewed, initiatives resulting from the strategy are run and progress is monitored by the Management Board. Our security strategy is aligned with overall business strategy and aims at:

- addressing customers' expectations who want to use secure software and have EG to protect their data being and acting as a business enabler,
- protecting EG customers, businesses and employees data and ensuring that they can continually rely on our services.

Cyber and information security policy

EG has drawn up and continuously maintains an overall cyber and information security policy ("Cyber and Information Security Policy") and supporting documents, based on security standards such as ISO 27001 and CIS Controls.

The overall security framework at EG consists of:

- cyber and information security policy,
- group-level policies, procedures and guidelines that apply to all EG companies and are available for all EG employees,
- local security procedures and instructions in the individual business units or at EG companies.

The security committee performs an annual assessment of the cyber and information security policy. Associated procedures and guidelines are periodically reviewed and maintained by the central security team. The aim of these assessments is to ensure that they meet the external obligations set out by law and contracts/agreements.

Access management

To manage access to the company's systems, information and networks, rules have been established for granting, changing and revoking access and rights to all EG systems. Access management has been implemented for the handling and approval of both internal and external user accesses.

In EG, we are following 'MFA everywhere' concept which assumes, that all employee accesses to company systems are only granted after successful validation using Multi-Factor Authentication (MFA).

User identities and accesses are managed through central identity directories. Access to EG systems is limited to employees with a work-related need based on their roles and responsibilities within the organization. The technical administration of accesses to EG's internal systems and data is managed by a corporate IT team.

Centrally managed vaults are used to securely store and manage passwords and secrets used to access systems used in EG. A password policy is defined following up-to-date security good practices to ensure that only strong passwords are configured in the systems.

Granting accesses must be approved by relevant managers or asset owners. Where required (sensitive privileges), user rights are periodically reviewed to ensure that only people with a work-related need have access to systems.

Users no longer having a work-related requirement for access are deactivated. All employees and external users' accesses are revoked when the employment terminates.

Encryption

A policy and a set of procedures have been developed to ensure relevant and necessary encryption of data. Encryption is used on external communication to and from the company and to and from data centres either through VPN solutions or SSL/TLS mechanisms. Encryption is applied when transmitting confidential or sensitive data through the internet, as well as when data are stored on laptops, mobile devices or removable media. Backups of the systems and data are also stored in an encrypted form.

External parties and supplier relationships

EG has formal procedures for entering into agreements and contracts with suppliers and consultants. These procedures ensure that the supplier meets the security obligations and requirements, in particular to which EG is subject through contracts and legislation. All new suppliers must be approved by the appointed body ("Vendor Approval Board"), which assesses the supplier's ability to meet applicable security and compliance requirements. Agreements are maintained through close dialogue and regular meetings with our suppliers. Supplier agreements are regularly optimised with respect to our situation and our customers.

Human resources security

The employees' security responsibilities are determined through an adequate job description and by the terms of the employment contract. Some employees are security cleared if there is a requirement agreed with a customer.

All employees receive mandatory training on security, which is conducted on a regular basis. Additionally, awareness is verified and increased through tests, such as simulated phishing campaigns.

All security guidelines and policies are available to the employees on EG's intranet. The individual employee is responsible for complying with the security policy. EG has internal procedures for handling employee violations of EG's security rules and procedures.

The employee is also responsible for reporting any breaches of security or suspicion of an incident. Information on how to notify and react to incidents is provided in the security documentation available to employees, as well as it is subject of the trainings provided to employees.

Network and office infrastructure security

Network and office infrastructure is based on modern state-of-the art solutions that are following EG global standard and are managed and secured according to global EG security standards. External boundary is secured with a firewall. Configuration of network devices is verified against compliance with global EG security standards based on Center for Internet Security (CIS) Benchmarks. Vulnerabilities in the systems are timely identified and remediated, and patches are timely applied. Administrative access to network devices requires MFA. Access to both WiFi and ethernet networks require device authentication with certificates. Least privilege principle is followed regarding access to the systems – default access is limited to basic office and intranet services and internet offered to all personnel, any additional access to business applications or systems requires a request and approval of appropriate system owners. Guest WiFi network is isolated from EG network. Physical security of devices and cabling is ensured.

Physical security

All office premises by default are accessible only for employees with valid cards and are equipped with standard office access control and anti-break-in measures. Guests require escort from employees and are registered. Clean-desk policy and locking of workstations are requirements for all employees stressed through policies and trainings. Network and office infrastructure (devices and cabling) are properly secured by placing in separate locked premises (devices) and proper routing (cabling).

Product security

Server infrastructure is managed and secured according to global EG security standards. Configuration of servers is verified against compliance with global EG security standards based on Center for Internet Security (CIS) Benchmarks. Server infrastructure is protected with leading endpoint detection and response solution. Vulnerabilities in the systems are timely identified and remediated, and patches are timely applied. Administrative access to servers and cloud infrastructure requires MFA, is logged and monitored. Least privilege principle is followed regarding access to the systems and access is limited only to authorized individuals. Security solutions are implemented to protect against network attacks, including distributed denial of service (DDoS) attacks. Physical and environmental security of the infrastructure is ensured in all data centers. Systems are regularly backed up and backups are protected in order to allow systems recovery in case it is needed.

Security controls are implemented into the software development lifecycle (SDLC). All code and software components used in EG's applications are scanned with leading security software to identify and fix vulnerabilities. Applications are also tested dynamically using automated solutions and through manual penetration tests conducted by central security team or external partners.

Security awareness program

In EG we are running an organization wide security awareness program to ensure that our employees are a vital part of our defense. Regular security awareness trainings for all employees, conducted at least quarterly, serve as the foundation of the EG's security awareness program. Apart from general awareness trainings addressed to all employees, group specific trainings are conducted to ensure that appropriate security knowledge and skills are possessed by relevant personnel. In particular, there are dedicated trainings addressed to engineers responsible for developing and maintaining EG's applications, to train them secure coding practices.

EG employees are regularly tested using simulated attacks to verify their capability to recognize, avoid, and report potential threats that can compromise data and systems. The awareness campaigns, trainings and simulated attacks are delivered using platforms developed by leading security organizations. There are also security training events organized by central security team.

Security incident management

All security incidents are handled according to established security incident management policy in EG ("Security Incident Management Policy") and procedures.

Central security team is responsible for developing and maintaining security incident management capabilities across EG, including development of policies, procedures and guidelines, organization of trainings and workshops, overseeing major security incident handling and building awareness among employees on how to act on incidents. Appointed security incident managers for all business units coordinate efforts related to security incident management within the different units and are responsible for ensuring that security incidents are handled according to the standards. If an employee becomes aware of a security incident or suspects it, he or she must report the case according to the procedures.

There is a dedicated process for handling major security incidents, which includes in particular setting up a major security incident team and reporting to the top management.

In the event of a security incident, the affected customers are notified as soon as possible, and steps are taken to minimize the impact of the incident.

Security monitoring

Effective monitoring of security events in the systems provides important information for both proactively and reactively being able to avoid security incidents that would otherwise affect confidentiality, integrity and availability of systems. The aim of the monitoring is to detect and respond to events before they have an impact on security of data and systems. To accommodate this, EG has established a partnership with a leading security vendor providing technology and services allowing to detect and respond to potential threats to our endpoints, data, identities, and networks. Security events in EG’s systems are continuously monitored in 24/7 model to ensure that suspicious activities are identified and responded as quickly as possible.

Workstations and mobile devices security

Workstations and mobile devices are following EG global standard and are managed and secured according to global EG security standards, based on Center for Internet Security (CIS) Benchmarks. The configuration is managed and monitored centrally, vulnerabilities are timely identified and remediated, and patches are timely applied. All workstations and mobile devices employ storage encryption. Data on external USB storage can be saved only if the storage is encrypted and USB drives are scanned for malicious files when connected to the workstation. Workstations are equipped with vulnerability scanning and endpoint detection and response solutions. Only software required for business purposes may be present on the workstations.

Security in EG – appendix regarding offices in India

Scope of operations and IT environment in India offices

Scope of work for EG personnel in India is focused mainly on support in maintenance and development of EG products and technologies shared across EG. All India personnel and operations are organized according to and using the worldwide EG security policies, standards, processes, and solutions. The security of India offices is managed by central EG security organization.

The IT environment in India is limited to office infrastructure and workstations, that are organized and managed in line with global EG security standards. There are no specific systems, applications, or repositories, where EG data would be processed, except for workstations, network equipment and print servers. Personnel are using global EG systems hosted centrally in European Economic Area (EEA) and cloud systems also selected and managed centrally by EG.

In case of our Indian personnel being engaged in any new activities or processes a Transfer Impact Assessment is performed.

Security measures applicable for offices in India

The specific security measures implemented in the offices in India are compliant with the global EG standards for offices and described in the following sections of this document:

- Network and office infrastructure security
- Workstations and mobile devices security
- Access management
- Human resources security
- Physical security