Externer Security Incident Management Prozess	External Security Incident Management Process
A. Geltungsbereich Die Umsetzung eines Security Incident Management (SIM) Prozesses sowie die Informationspflichten sind zwingend erforderlich für Geschäfts- und Kooperationspartner der ERGO Group, die sensible Daten im Sinne der DSGVO sowie gemäß der internen Einstufung der ERGO Group verarbeiten. Zudem ist die Umsetzung für Geschäfts- und Kooperationspartner mit einer direkten technischen Verbindung (z. B. VPN- oder SFTP-Verbindungen) zur ERGO Group verpflichtend. Geschäfts- und Kooperationspartner, die nur Active Directory Konten der ERGO Group verwenden, aber keine Daten auf eigenen System verarbeiten, müssen keinen SIM Prozess umsetzen, aber die Informationspflichten erfüllen.	**A. Scope** The implementation of a Security Incident Management (SIM) process as well as the information duties are mandatory for business and cooperation partners of the ERGO Group who process sensitive data in the sense of the GDPR and in accordance with the internal classification of the ERGO Group. Furthermore, the implementation is mandatory for business and cooperation partners with a direct technical connection (e.g. VPN or SFTP connections) to the ERGO Group. Business and cooperation partners who only use Active Directory accounts of the ERGO Group but do not process data on their own system do not have to implement a SIM process, but must fulfill the information requirements.
B. Einleitung Firmen befinden sich heute stärker denn je im Fokus von Computer-Angriffen. Die spektakulärsten bzw. schwerwiegendsten dieser Angriffe werden immer wieder in der tagesaktuellen Berichterstattung thematisiert. Häufig handeln die Berichte von Ransomware-Angriffen, der Veröffentlichung von gestohlenen Daten oder aber von größeren finanziellen Schäden. Klar ist jedoch, dass die meisten dieser Angriffe unerwähnt bleiben und auch, dass Angriffe jeden treffen können. So verwenden Angreifer z. B. E-Mails mit maliziösen Anhängen, um Schad-Software auf einem Benutzersystem zu installieren. Anschließend nutzt die Schad-Software Mechanismen zur Rechteerweiterung sowie zur weiteren Verbreitung auf andere Systeme. Je nach Ziel der Angreifer werden anschließend z. B. Daten extrahiert und an den Angreifer gesendet oder aber infizierte Computersysteme verschlüsselt. Das Potenzial solcher Angriffe beschränkt sich dabei nicht nur auf die zuerst angegriffene Firma. So kann es zum Beispiel in der Verbreitungsphase einer Schad-Software dazu kommen, dass angeschlossene Geschäftspartner, Kunden oder Kooperationspartner ebenfalls von der Schad-Software befallen werden. Um dieser Bedrohung zu begegnen, ist es essenziell, entsprechende Prozesse zur Abwehr von Angriffen zu implementieren. Zudem ist es notwendig, eine entsprechende Kommunikation mit Geschäftspartner, Kunden und Kooperationspartner im Falle eines Angriffes zu etablieren, um diese im Fall eines Angriffs vor den Auswirkungen zu schützen.	**B. Introduction** Today companies are more than ever in the focus of computer attacks. The most spectacular or serious of these attacks are always the subject in the daily news. Often the news report from ransomware attacks, the publication of stolen data or major financial damages. However, it is clear that most of these attacks go unmentioned and that attacks can affect anyone. For example, attackers use e-mails with malicious attachments to install malicious software on a user system. The malicious software then uses mechanisms to extend rights and to spread further to other systems. Depending on the target of the attackers, data is then extracted and sent to the attacker or infected computer systems are encrypted. The potential of such attacks is not limited to the first attacked company only. For example, during the distribution phase of a malicious software it can happen that affiliated business partners, customers or cooperation partners are also attacked by the malware. To counter this threat, it is essential to implement appropriate processes to defend against attacks. In addition, it is necessary to establish appropriate communication with business partners, customers and cooperation partners in case of an attack in order to protect them from the effects of an attack. It should also be mentioned that the supervisory authorities also require corresponding processes.

Es sollte auch nicht unerwähnt bleiben, dass entsprechende Prozesse auch von den Aufsichtsbehörden gefordert werden.	
C. Security Incident Management (SIM) Prozess Auf dieser Basis wird daher gefordert, dass Lieferanten (wie im Geltungsbereich definiert), einen angemessenen Security Incident Management (SIM) Prozess implementieren und leben. Als angemessen erachtet werden hierbei die gängigen SIM-Prozess-Standards der Industrie bzw. der Aufsichtsbehörden. Dies sind z. B. die SIM-Prozesses nach • NIST |1| • SANS |2| |3| • Bundesamt für Sicherheit in der Informationstechnik |4| • Carnegie Mellon University |5| • ISO 27001 A.16 Typischerweise enthalten die Prozesse dabei z. B. folgende Phasen: • Identifizierung, Benachrichtigung und Vorbewertung • Bewertung • Eindämmung, Reaktion und Beweiserhebung (Forensik) • Wiederherstellung der betroffenen Services • Nachbearbeitung Die Ausgestaltung und die Einteilung der einzelnen Phasen variiert innerhalb der oben genannten SIM-Prozesse dabei unwesentlich und die hier aufgelisteten Phasen können zwischen den Prozessen abgebildet werden. Daher gilt ein eigener entwickelter SIM-Prozess als ausreichend, sofern er sich ohne den Verlust wichtiger Schritte auf einen solchen Standard-Prozess abbilden lässt. Sofern eine Abbildung auf einen der Standard-Prozesse nicht offensichtlich ist, sollten vorhandene Prozesse um eine entsprechende Erklärung ergänzt werden.	**C. Security Incident Management (SIM) Process** On this basis, it is therefore required that suppliers (as defined in the scope) implement and live an appropriate Security Incident Management (SIM) process. The common SIM process standards of the industry and regulatory authorities are considered appropriate. These are, for example, the SIM process according to • NIST|1| • SANS |2| |3| • Federal Office for Information |4| • Carnegie Mellon University |5| • ISO 27001 A.16 Typically, the processes contain e.g. the following phases: • Identification, notification and pre-evaluation • Evaluation • Containment, response and evidence gathering (forensics) • Restoration of the affected services • Post processing The design and classification of the individual phases varies insignificantly within the above-mentioned SIM processes and the phases listed here can be mapped between the processes. Therefore, a SIM process developed in-house is sufficient, if it can be mapped to such a standard process without losing important steps. If mapping to one of the standard processes is not obvious, existing processes should be supplemented by a corresponding explanation.
D. Informationspflichten Wie bereits oben beschrieben, kann ein Vorfall auch Auswirkungen auf die Sicherheit der Computer-Netze von Geschäftspartnern, Kunden und Kooperationspartnern haben. Um das Risiko für die ITERGO und auch deren Geschäftspartner, Kunden und Kooperationspartner so gering wie möglich zu halten, muss eine Meldung eines schwerwiegenden Sicherheitsvorfalls an die ERGO Group erfolgen, wenn • das Risiko besteht, dass eine Schad-Software aus einem Sicherheitsvorfall das Computer-Netz der ERGO Group angreifen könnte.	**D. Information requirements** As described above, an incident can also affect the security of the computer networks of business partners, customers and cooperation partners. To keep the risk for ITERGO and also its business partners, customers and cooperation partners as low as possible, a report of a serious security incident must be made to the ERGO Group if • there is a risk that malware from a security incident could attack the ERGO Group's computer network.

• das Risiko besteht, dass Mitarbeiter einen Vorfall aus der Firma auf die ERGO Group übertragen könnten. • damit zu rechnen ist, dass die ERGO Group aufgrund eines Sicherheitsvorfalls nachfolgend das Ziel von Angriffen werden könnte. • personenbezogene Daten der ERGO Group von einem Angriff betroffen sein könnten. • die Vertraulichkeit, Verfügbarkeit oder Integrität von ERGO Group Daten betroffen sein könnte. • es aufgrund des Sicherheitsvorfalls zu Medienberichten kommen könnte, die einen Reputationsschaden für die ERGO Group bedeuten. Typische Szenarien für eine Benachrichtigung sind z. B. • Ransomware-Vorfälle • Vorfälle mit Schad-Software, die das Potential haben sich auszubreiten • der Abfluss von personenbezogener Daten Die ERGO Group empfiehlt, die Ausarbeitung entsprechender Verteilerlisten für die Benachrichtigung im Falle eines Sicherheitsvorfalles im Vorfeld. Bei einer Meldung eines Sicherheitsvorfalls werden dabei mindestens die folgenden Angaben erwartet: • Wann hat der Sicherheitsvorfall stattgefunden? • Wer meldet den Sicherheitsvorfall (Name, Firma, Adresse, Telefonnummer, E-Mail-Adresse) • Worum handelt es sich bei dem Sicherheitsvorfall (kurze Beschreibung des Vorfalls und der zu erwartenden Auswirkungen) • Was war die Ursache für den Sicherheitsvorfall? • Sind personenbezogene Daten betroffen? Falls ja: Wurde bereits eine Meldung an die Datenschutzbehörden durchgeführt? • Welches potentielle Risiko besteht für Geschäftspartner, Kunden und Kooperationspartner • Informationen zum Schutz, z. B. Indicator of Compromise[1], Bereitstellung von Malware-Samples • Zeitpunkt des nächsten zu erwartenden Updates • Kontaktpunkt für dringende Fragen Da es im Rahmen von Sicherheitsvorfällen typischerweise nicht möglich ist, die Fragen aller Geschäftspartner, Kunden und Kooperationspartner	• there is a risk that employees could transfer an incident from the company to the ERGO Group. • it is to be expected that the ERGO Group could subsequently become the target of attacks due to a security incident. • personal data of the ERGO Group could be affected by an attack. • the confidentiality, availability or integrity of ERGO Group data could be affected. • the security incident could result in media reports that could damage the reputation of the ERGO Group Typical scenarios for a notification are • Ransomware attacks • Incidents with malicious software that have the potential to spread • the leakage of personal data The ERGO Group recommends that appropriate distribution lists for notification in the event of a security incident are compiled in advance. When a security incident is reported, at least the following information is expected: • When did the security incident occur? • Who reports the security incident (name, company, address, phone number, e-mail address) • What is the security incident about (brief description of the incident and expected effects) • What was the reason for the security incident? • Is personal data affected? If so, have you already informed the data protection authorities? • What are the potential risks for business partners, customers and cooperation partners? • Information to support the protection of ERGO Group, e.g. Indicator of Compromise[1], provision of malware samples • Time of the next expected update • Contact point for urgent questions As it is typically not possible to answer the questions of all business partners, customers and cooperation partners at the same time in the context of security incidents, the ERGO Group recommends providing appropriate information in the form of a circular e-mail or press release. In addition, in the event of a security incident, consider conference calls at short notice or the rapid production of a podcast. We recommend to set up a Single Point of Contacts (SPOC) to ensure efficient communication. In

[1] Indicator of Compromise (IoC) sind Merkmale, die auf Kompromittierung eines Computersystems oder Netzwerks hinweisen, z. B. URLs von maliziösen Servern / Indicators of Compromise (IoC) are information that indicate the compromise of a computer system or network, e.g. URLs of malicious servers.

gleichzeitig zu beantworten, empfiehlt die ERGO Group die Bereitstellung entsprechender Informationen in Form einer Rundmail oder Presseerklärung. Zudem sollte im Fall eines Sicherheitsvorfalls über die kurzfristige Einberufung von Telefonkonferenzen oder die schnelle Produktion eines Podcast nachgedacht werden. Es wird auch die Einrichtung eines Single Point of Contacts (SPOC) empfohlen, um eine effiziente Kommunikation zu gewährleisten. Zudem empfiehlt die ERGO Group mindestens eine tägliche Aktualisierung der bereitgestellten Informationen. Die Meldung eines Sicherheitsvorfalls an die ERGO Group entbindet nicht von einer ggf. notwendigen Meldung an andere Behörden wie z. B. der Datenschutzbehörde. Diese Meldepflichten sind weiterhin eigenständig von Geschäfts- und Kooperationspartnern zu erfüllen.	addition, the ERGO Group recommends at least a daily update of the information provided. Reporting a security incident to the ERGO Group does not release your company from the obligation to report the incident to other authorities, such as the data protection authority, if necessary. Business and cooperation partners must fulfill these reporting obligations independently.
E. Kontaktinformationen Im Fall eines schwerwiegenden Sicherheitsvorfalls mit evtl. Bezug zur ERGO Group wenden sich Geschäfts- und Kooperationspartner mit Zugang zum Helpdesk bitte an diesen. Geschäfts- und Kooperationspartnern ohne Zugang zum Helpdesk wenden sich im Fall eines schwerwiegenden Sicherheitsvorfalls mit evtl. Bezug zur ERGO Group bitte an: • csirt@itergo.com • +49 211 477 4700	**E. Contact information** In the event of a serious security incident possibly relating to the ERGO Group, business and cooperation partners with access to the helpdesk should contact the helpdesk. Business and cooperation partners without access to the helpdesk should contact the ERGO Group in the event of a serious security incident with possible reference to the ERGO Group using the following contact: • csirt@itergo.com • +49 211 477 4700
F. Verweise https://www.nist.gov/publications/computer-security-incident-handling-guide https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791 https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2020.pdf?__blob=publicationFile&v=1 https://www.cmu.edu/iso/governance/procedures/IRPlan.htmlInternet Explorer	**F. References** https://www.nist.gov/publications/computer-security-incident-handling-guide https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791 https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2020.pdf?__blob=publicationFile&v=1 https://www.cmu.edu/iso/governance/procedures/IRPlan.html

Compromise (IoC) are information that indicate the compromise of a computer system or network, e.g. URLs of malicious servers