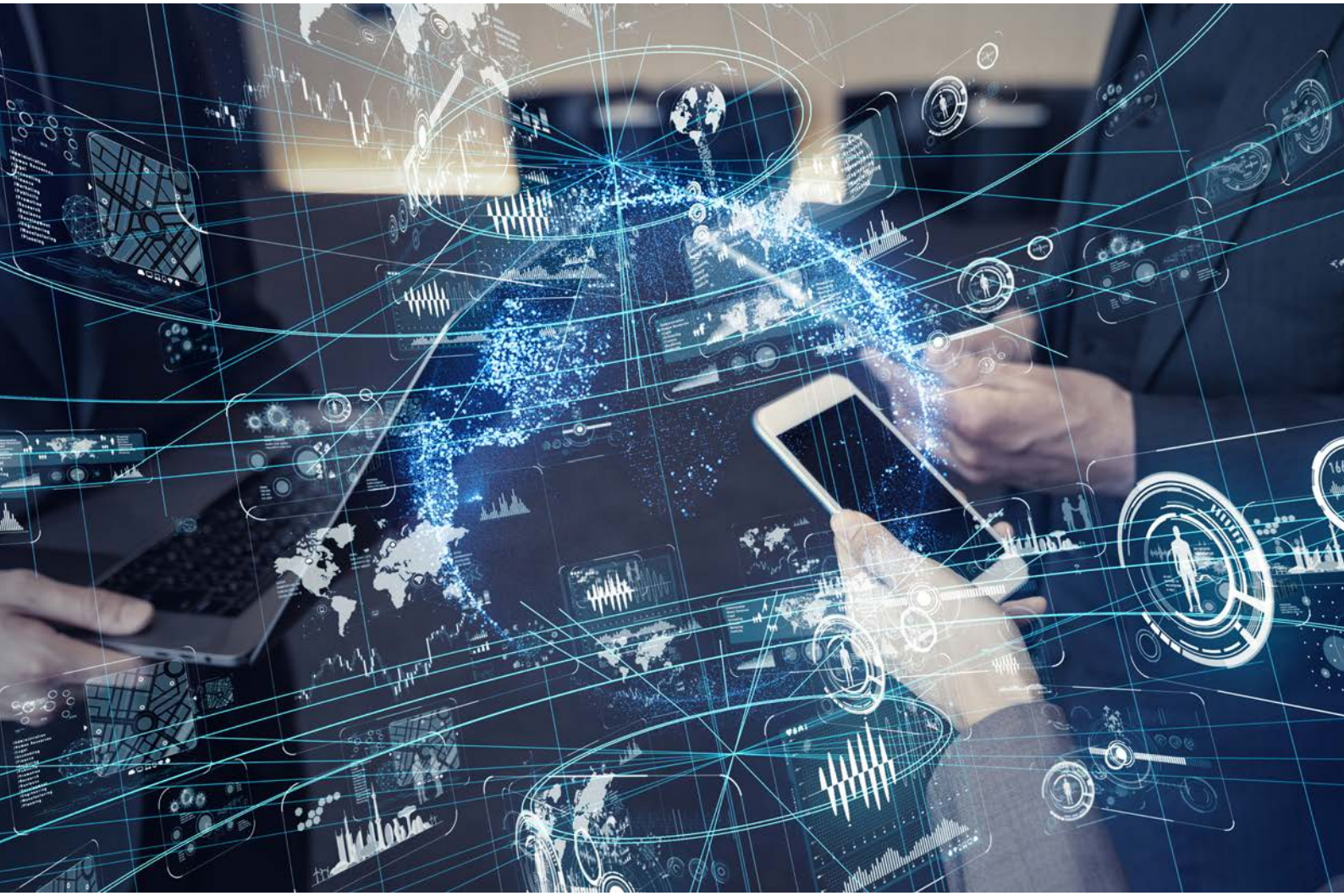
DOLPHIN
an F24 company

DOLPHIN SYSTEMS WHITEPAPER

Cyber Resilience

Überleben in der IT-Krise



Überleben in der IT-Krise durch Cyber War Games

Es ist eine Frage der Zeit bis Ihr Unternehmen in einer IT-Krise steckt! Unbegründete Angstmacherei? Vielleicht stecken Sie inmitten einer IT-Krise und Sie haben es noch gar nicht bemerkt. Denn Sie wissen gar noch nicht, dass vertrauliche Informationen oder Identitäten gestohlen oder kompromittiert wurden. Sie wissen nicht, dass Ihre IT-Systeme infiziert sind und Sie ausspäht werden? Sie wissen auch nicht, dass Ihre Informationen im Darknet zum Verkauf angeboten werden? Sehr wahrscheinlich wissen Sie auch nicht, wer Sie angreift oder ausspioniert.

Und plötzlich ist die Krise bittere Realität. Trotz vielfältiger Schutzmassnahmen und Mitarbeitertrainings ist das Unternehmen Opfer eines massiven Hacker-Angriffs geworden. Heikle Kundendaten sind abhandengekommen, zudem wurden finanzielle Informationen abgeändert und verfälscht – und das bereits seit Wochen oder Monaten.

Die Verwundbarkeit eines Unternehmens steigt exponentiell! Der Phänomenbereich Cybercrime ist, wie der gesamte Bereich der Informationstechnik, von einer hohen Dynamik in der Entwicklung geprägt.

Aus der Krise wird so leicht eine Katastrophe mit Folgekosten in Millionenhöhe, die das Überleben der Firma gefährden. «Viele Konkurse hätten schon verhindert werden können, wenn die Unternehmen genügend in ihre Sicherheit und in ein professionelles Krisenmanagement investiert hätten», behauptet Richard Werner, Geschäftsführer von Risk Control RCC.

Während allgemein die Straftaten in der Schweiz gemäss der jüngsten polizeilichen Kriminalstatistik (PKS) rückläufig sind, steigen die computerkriminellen Straftaten.

Zu den häufigsten diesbezüglichen Straftaten gehört der «betrügerische Missbrauch einer Datenverarbeitungsanlage» nach Artikel 147 des Schweizerischen Strafgesetzbuchs (StGB). Hier zählt die PKS 4956 Fälle. Das sind 4 Prozent mehr als 2016. Ebenfalls gestiegen sind die unbefugte Datenbeschaffung (Art. 143 StGB) und das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB). So stieg Ersteres von 975 auf 1063 Fälle, was einem Plus von 9 Prozent entspricht. Beim Hacking-Strafbestand wurden 2017 dagegen 404 Fälle gezählt. Dies entspricht einem Plus von 5 Prozent gegenüber 2016. Allgemein lässt sich der Statistik entnehmen, dass die Aufklärrate relativ gering ausfällt. Sie schwankt zwischen 20 und 25 Prozent. Gemäss BKA-Lagebild wurden 2017 insgesamt 85'960 Fälle von Cybercrime im engeren Sinn erfasst und 251'617 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten. So wurde beispielsweise die Softwaremanipulation von ca. 1,3 Mio. DSL-Routern eines deutschen Internetproviders durch Malware im November 2016 – trotz einer siebenstelligen Anzahl von Geschädigten – als nur ein Fall der Computersabotage in der PKS ausgewiesen. Die Zunahme bei mobiler Malware wurde mit + 54 % angegeben.

VERALTETE POLIZEISTRUKTUREN

Cyber-Ermittlungen scheitern oftmals bereits an Grenzen. Fast immer führen die Spuren ins Ausland. Kurz: Für die komplexen Ermittlungen von heute sind die Strukturen aus dem letzten Jahrhundert veraltet. «Wir bekämpfen die Kriminalität des 21. Jahrhunderts mit einer Organisation des 19. Jahrhunderts.» Verbrecher orientieren sich immer weniger an territorialen Grenzen und agieren extrem schnell. Cyberkriminelle reagieren rasch auf Trends, wechseln Plattformen, Vorgehen und Operationsbasis. Hinzu kommt, dass die Täter in der digitalen Welt ihre Spuren rasend schnell verwischen. Die Polizeistrukturen müssen im Kampf gegen Cyberkriminelle ohne Rücksicht auf althergebrachte Zuständigkeiten angepasst werden. Die Ermittler stehen unter enormen Druck. Eine neue Plattform unter dem Titel Cyberboard soll die Akteure zusammenführen. So banal viele Täuschungsmanöver aus der Ferne erscheinen mögen: Sie bringen die Polizei rasch an Grenzen. Und während die Herausforderungen für die Polizei sukzessive (und nicht nur im Bereich der Cyberkriminalität) grösser werden, liegt ein ressourcenmässiger Ausbau vielerorts nicht drin.

IST IHRE ITC-SICHERHEITSKONZEPT UND IHR KRISENMANAGEMENT SICHER UND SCHLAGKRÄFTIG GENUG, UM MIT AUFKOMMENDEN BEDROHUNGEN FERTIG ZU WERDEN?

Cyberkriminelle nutzen oft Schwachstellen in Applikationen. Sie fokussieren sich immer stärker auf menschliches Fehlverhalten anstatt auf technische Fehler, um an Geld, persönliche Daten oder geistiges Eigentum zu gelangen. Die Motivation für Angriffe ist meist Geld.

CYBERCRIME: WIE DIE TÄTER IM NETZ ANGREIFEN

Cybercrime hat viele Formen. Hier eine Übersicht über die gängigsten Phänomene.
Heute unterscheidet man zwischen digitalisierter Kriminalität und Cybercrime im engeren Sinn.
Zur ersten Kategorie zählt man klassische Delikte, die unter Zuhilfenahme des Internets und sozialer Netzwerke verübt werden: zum Beispiel eine Drohung via Facebook oder Whatsapp.
Cybercrime im engeren Sinn meint Straftaten gegen das Internet und seine Instrumente. Darunter fällt zum Beispiel die Infizierung eines Computers mit Software, die den Nutzer ausspäht. Es gibt aber auch Mischformen.

DAS BUNDESAMT FÜR POLIZEI UNTERSCHEIDET MEHR ALS 20 PHÄNOMENE VON CYBERCRIME – ZUM BEISPIEL:

- **Phishing:** Kriminelle bringen trickreich Passwörter in Erfahrung – zum Beispiel mit gefälschten Mails oder Websites. Auch an weiteren persönlichen Daten wie Name, Geburtstag, Anschrift oder Online-Banking-Zugangsdaten sind sie interessiert. Mit diesen Daten können sie Missbrauch betreiben und im Namen des Opfers Geschäfte abwickeln.

- **Romance Scam:** Romance Scammer eröffnen auf Singlebörsen gefälschte Profile und werben so um ihre Opfer. Sie gaukeln vor, sich verliebt zu haben, und stellen Treffen in Aussicht. Sobald die Opfer, bei denen es sich in der Regel um Frauen handelt, Gefühle entwickeln, werden sie ausgenutzt und betrogen: Meist werden die Opfer aufgefordert, Geld zu überweisen. Romance Scammer sind meist in Banden organisiert. Im Jahr 2016 wurden dem Bundesamt für Polizei (Fedpol) 140 Fälle gemeldet.

- **Police Ransomware:** Eine Schadsoftware blockiert den Computer. Es erscheint eine vermeintlich behördliche Mitteilung, welche die betroffene Person zur Bezahlung einer Busse auffordert, damit der Computer wieder entsperrt wird. Infizierte Systeme werden oftmals vollständig verschlüsselt und gesamte Netzwerke erheblich gestört. Betroffene, die ihre IT-Infrastruktur nicht durch aktuelle Backups wieder aufbauen können, erleiden massive Beeinträchtigungen bis hin zu einem kompletten Ausfall des Geschäftsbetriebs. Angesichts dieses hohen Schadenpotenzials zahlen zahlreiche Geschädigte die vergleichsweise niedrigen geforderten Lösegelder.

Aus polizeilicher Sicht ist von entsprechenden Zahlungen abzuraten, da hierdurch das kriminelle Geschäftsmodell Ransomware unterstützt wird und Anreize zur weiteren Tatbegehung geschaffen werden. Dies insbesondere vor dem Hintergrund, dass möglicherweise der Betroffene selbst gegen die Infizierungen vorgehen kann: Bei Betroffenheit durch Ransomware empfiehlt sich eine „Open-Source-Recherche“ nach frei verfügbaren Entschlüsselungstools, so beispielsweise über das von Europol und der niederländischen Cybercrime-Dienststelle (NHTCU) in Zusammenarbeit mit der Privatwirtschaft initiierte Projekt www.nomoreransom.org.

- **Spyware:** Die klassische Spyware wird dazu eingesetzt, Passwörter und Zugangsdaten zu erhalten, um finanziellen oder anderen Schaden anzurichten. Spyware wird in der Regel beim Surfen auf dubiosen Websites, durch Herunterladen von falscher Sicherheitssoftware, Öffnen von infizierten Anhängen oder direkt mittels Öffnen einer Datei, die auf einem Datenträger gespeichert ist, übertragen.

- **DDoS-Angriff:** DDos-Angriffe (Distributed Denial of Service) funktionieren mit der Versendung einer sehr grossen Anzahl von Anfragen (Datenpaketen) an einen Server, welcher eine Internet-Dienstleistung beherbergt. Dadurch ist er nicht mehr in der Lage, andere Anfragen zu beantworten, und der Dienst ist für legitime Nutzer nicht erreichbar. Solche Angriffe haben verschiedene Motive: So werden die Opfer erpresst, indem die Einstellung der Angriffe gegen Geld in Aussicht gestellt wird. Die Sperrung von gewissen Informationen kann aber auch politische oder religiöse Hintergründe haben.

- **Identitätsdiebstahl:** Freundschaftsanfragen von Bekannten auf Facebook, die sich als Fake herausstellen, kennt fast jeder: Die Betrüger sammeln und kopieren im Internet (meist) frei zugängliche Daten und Fotos des Opfers. Mit diesem Material erstellen sie ein Profil. Meist werden solche Profile als Vorbereitungshandlung zu einem Delikt gesammelt. Mit der fremden Identität können zum Beispiel Konten auf verschiedenen Plattformen eröffnet, Waren bestellt oder Aufträge erteilt werden.

Hand aufs Herz, wer hat sich vor einigen Jahren mit solchen Themen herumgeschlagen? Was wird wohl die Zukunft bringen?

FAKT IST:

- Eine grosse Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinaus und wird von den Geschädigten nicht bemerkt, die betroffenen Personen erkennen nicht, dass sie Geschädigte einer Cyber-Straftat geworden sind (z.B. bei Diebstahl der Identität bei einem Online-Shop) bspw. durch die Nutzung von technische Geräten, die unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht werden (z. B. Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen oder Infektion mit Cryptomining-Malware).

- Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. blosser Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z. B. Versicherung) reguliert wird

- Geschädigte, insbesondere Firmen, zeigen erkannte Straftaten nicht an, um beispielsweise im Kundenkreis die Reputation als «sicherer und zuverlässiger Partner» nicht zu verlieren.

- Geschädigte erstatten beispielsweise in Erpressungsfällen oftmals nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.

SCHÄTZEN SIE DIE SICHERHEIT IHRER IT IN IHREM UNTERNEHMEN RICHTIG EIN?

Seien Sie misstrauisch! Welche Risiken bestehen genau im aktuellen System? Was sind die besonders schützenswerten Daten? Sind im Unternehmen die Pläne für die digitale Transformation bereits erstellt?

FAKT IST:

- Das Unternehmen kann aufgrund eines erfolgreichen Cyber-Angriffs viel Geld, viele wertvolle Informationen und noch mehr Reputation verlieren!

- Eine Person klickt immer: 75 % der von Ransomware betroffenen Unternehmen infizierten sich in den letzten sechs Monaten durch schadhafte Mail-Anhänge.

WIE KANN DAS UNTERNEHMEN UMFASSEND GESCHÜTZT WERDEN?

1. Ein fundiertes Krisenmanagementkonzept und eine schlagkräftige jedoch schlanke Krisenorganisation ist überlebenswichtig. Jährliche Krisenübungen, auch War Games genannt, mit gut vorbereiteten Drehbüchern sollten erstellt werden. In solchen Drills werden mögliche Krisenszenarien simuliert, um die Unternehmensleitung und Mitarbeiter auf den Krisenfall vorzubereiten, damit auch bei einer reelen Cyberbedrohung das gesamte Unternehmen handlungsfähig bleibt.

2. Geschäftskontinuitätsplanung/Business Continuity Management (BCM) ist das Zauberwort. Unternehmen, die kein geeignetes Business Continuity Konzept implementiert haben, werden zweifellos das Nachsehen haben. Die Durchführung einer Geschäftsauswirkungsanalyse (Business Impact Analyse) mit der Definition der geschäftskritischsten Risiken wird für jedes Unternehmen zum entscheidenden Erfolgsfaktor. Das BCM-Konzept in Verbindung mit einem schlagkräftigen Krisenmanagement-Konzept und einer professionellen Krisenkommunikation hilft Ihrem Unternehmen, nach einer IT-Krise zu überleben und Ihre gute Reputation zu bewahren.

3. Die Durchführung eines Cyber Security Assessment empfiehlt sich. Damit werden Zweifel ausgeräumt und ermittelt, wo in der bestehenden IT-Landschaft potenzielle Sicherheitsrisiken bestehen. Die Information über Gegenmassnahmen, die umfassenden Schutz bieten, ohne die Produktivität des Unternehmens zu beeinträchtigen, sind ebenfalls wichtige Grundlagen. Die IT-Landschaft verändert sich aufgrund neuer Anforderungen ständig. Durch die Digitalisierung werden geschäftskritische Elemente zunehmend von IT-Prozessen und der Infrastruktur abhängig. Deshalb ist es entscheidend, dass die IT-Systeme geschützt und Sicherheitslücken möglichst vermieden werden. Ein Cyber Security Assessment schärft das Risikobewusstsein. Dies erleichtert es dem Unternehmen, Massnahmen zu evaluieren und umzusetzen. Falls beispielsweise eine Cyber-Security-Versicherung in Betracht gezogen wird, ist eine Analyse der Ist-Situation und die Einführung passender Massnahmen unabdingbar, um ein günstiges Produkt zu finden.

TECHNISCHE MASSNAHMEN

Zur Sicherstellung der IT-Sicherheit im Unternehmen sollten folgende Massnahmen berücksichtigt werden:

- Regelmässige Tests auf bekannte Schwachstellen in der eigenen ITC-Infrastrukturumgebung und bei Webapplikationen
- Sicherstellung der Aktualität der eigenen Infrastruktur
- Verbesserung der Anti-Phishing-Infrastruktur
- Berücksichtigung von Cyberrisiken in der Notfall- und Krisenplanung
- Krisenübung: Szenario eines Cyberangriffs simulieren, um die Sicherheitsbereitschaft des Unternehmens zu testen (Intrusion Detektion)
- Implementierung eines professionelles Alarmierungssystem, um rechtzeitig auf Bedrohungen reagieren zur können und handlungsfähig zu bleiben.
- Erstellung eines Business Continuity Management Konzepts.

AWARENESS TRAINING (AUSBILDUNGSKONZEPT) INFORMATIONSSICHERHEIT

- Sensibilisierung der Mitarbeiter und der Geschäftsleitung
- Installation eines aktuellen e-Learning Programms für alle Mitarbeiter
- Regelmässige Mitarbeiter-Information vor aktuellen Bedrohungen und über wichtige Verhaltensanweisungen
- Emotionalisierung der Mitarbeiter (Vermittlung einer positiven Einstellung zum Thema Sicherheit)
- Motivation der Mitarbeiter (einen Anreiz zur Verhaltensänderung bieten)
- Berücksichtigung des Faktor Mensch beim Schutz des Unternehmens vor Informationssicherheits-Risiken.

Fazit

Die zunehmende Bedeutung der IT für Unternehmen, Behörden und für den privaten Bereich steigert die Manipulations- und Angriffsmöglichkeiten. Aktuelle Technologietrends eröffnen neue Tatgelegenheiten und dürften die Bedrohungslage weiter verschärfen. Dabei rücken mobile Endgeräte, deren Schutz von den Nutzern oftmals vernachlässigt wird, besonders in den Fokus. Aus den genannten Gründen müssen die Nutzer von Smartphones, Tablets und Smart Home-Technologien weiter sensibilisiert werden. Ist das Unternehmen gegen einen Cyber-Angriff wirklich gewappnet? Wie reagieren Mitarbeiter und Management, wenn Hacker einmal richtig zuschlagen sollten? Antworten auf solche Fragen liefern Krisenübungen, sogenannte War Games.

Die Erstellung und die Pflege eines Krisenmanagementkonzepts wie auch das Trainieren der gesamten Krisenorganisation im Unternehmen sind die wichtigen Pfeiler der IT-Sicherheit. Die Implementierung eines geeigneten Business Continuity Konzepts und die Durchführung eines unabhängigen Cyber Security Assessments stärkt das Unternehmen mit passenden Massnahmen die IT-Systeme und schützt vor Cyber-Angriffen.

Richard WERNER - Dr. MBA
Seit 2003 ist er General Manager der Risk Control RCC GmbH und seit 2013 Vorstandsmitglied der Non Profit Genossenschaft Private & Confidential Group. Er besitzt 20-jährige, internationale Erfahrung in Aufbau und Implementierung von integralen Notfall-/Krisen- und Business-Continuity-Management-Führungssystemen.

Experte in Krisenkommunikation und Reputationsmanagement. Tätigkeit als Fachreferent an verschiedenen Fachhochschulen und Universitäten. Mehrjährige Tätigkeiten als Risk Officer bei renommierten Schweizer Blue-Chip-Unternehmen.

Quellenangaben:
Bundeskriminalamt BKA, Cybercrime Bundeslagebild 2017
Die Krise als Übung, Risk Control RCC, Dr. Richard Werner MBA 2016
Neue Zürcher Zeitung NZZ 2.2.2018 «Die Kriminalität im Internet nimmt zu – die Schweiz plant mehrere Cybercrime-Zentren, Daniel Gerny
Melde- und Analysestelle Informationssicherung (MELANI)
Bundesamt für Polizei (FEDPOL)
Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
Bundesamt für Sicherheit in der Informationstechnik BSI

Wie Sie FACT24 bei der erfolgreichen Bewältigung von Cyber Incidents oder Krisenszenarien unterstützt.

WENN IT-SYSTEME AUSFALLEN, STEHT FÜR EIN UNTERNEHMEN VIEL AUF DEM SPIEL.

- IT-Sicherheit ist für digitalisierte Unternehmen eine Top-Priorität, da die hochgradige Vernetzung und Komplexität der Systeme ihren gesamten Wertschöpfungsprozess verletzlicher und angreifbarer macht.

- Unternehmen müssen sich auf diese Risiken mit technisch-organisatorischen Massnahmen einstellen und ihr Alarmierungs- und Notfallmanagement bereits im Vorfeld einer Krise richtig aufstellen.

- Im akuten Krisenfall müssen Unternehmen verschiedene gesetzliche Meldepflichten fristgerecht einhalten, um Sanktionen von Aufsichtsbehörden zu vermeiden– beispielsweise Geldbussen.

MIT EINEM GUT AUFGESTELLTEN ALARMIERUNGS- UND NOTFALLMANAGEMENT KÖNNEN SIE DIE KRISE GEZIELTER UND SCHNELLER BEWÄLTIGEN UND FOLGESCHÄDEN EINDÄMMEN.

KOMMUNIZIEREN

Alarmieren und informieren Sie auf Knopfdruck alle relevanten Stakeholder automatisiert und über mehrfach redundante Kanäle.

MANAGEN UND MONITOREN

Behalten Sie stets den Überblick – alle relevanten Informationen stehen Ihnen auf Ihrem Krisenmanagement Dashboard zur Verfügung. Dank Software-as-a-Service (SaaS) sind Sie von Ihrer IT-Infrastruktur vollkommen unabhängig und bleiben so jederzeit handlungsfähig.

DOKUMENTIEREN

Alle Vorgänge werden automatisch revisionssicher dokumentiert – greifen Sie in Echtzeit auf Daten zur Analyse oder zur Beweissicherung zurück.

IM ERNSTFALL TICKT DIE UHR:

Je länger eine Lieferkette oder die Fertigung unterbrochen wird, desto höher können die Umsatzverluste ausfallen. Überdies steht nicht nur die Reputation eines Unternehmens auf dem Spiel, weil möglicherweise wichtige Sicherheitsmassnahmen nicht getroffen wurden. Auch staatliche Sanktionen wie Bussgelder sind möglich, wenn bestimmte Meldepflichten versäumt werden. Das Unternehmen sollte deshalb im Vorfeld sein Notfall- und Krisenmanagement richtig aufstellen, indem es Sofortmassnahmen festlegt.

Ziel ist es, die Ursache der Störung zu identifizieren und zu beheben, die Integrität der Daten zu schützen und die Arbeitsfähigkeit des Unternehmens wiederherzustellen

IM ERNSTFALL TICKT DIE UHR! VORBEREITUNG AUF DEN TAG X IM ÜBERBLICK

- Verantwortlichkeit und Rolle festlegen
- Arbeitsabläufe definieren
- Kommunikation standardisieren
- Kommunikation übersichtlich und resilient gestalten
- Informationsströme kanalisieren und absichern
- Den Notfall üben
- Protokollierung sicherstellen

TIPP: AUF CYBERATTACKEN GUT VORBEREITET SEIN

Ziel muss es sein, ungewöhnliche Vorkommnisse schnell erkennen, analysieren und somit unterbinden zu können. Ausserdem sollen die Folgekosten durch zu lange Systemausfälle minimiert werden. Im Ernstfall muss das Alarmierungs- und Meldesystem die richtigen Personen und Stellen benachrichtigen, damit das Unternehmen die Krise nicht nur so schnell wie möglich bewältigen, sondern auch gesetzliche Meldepflichten einhalten kann.

Technisch-organisatorische Massnahmen nach Stand der Technik sicherstellen.	**Alarmierungs- und Meldesystem definieren und aufsetzen.**	**Notfallmanagement etablieren.**	**Qualifizierte Personalressourcen bereitstellen.**

Erfahren Sie mehr zum Thema in unserem Whitepaper «IT-Security – Im Falle eines Cyberangriffs weiterhin verlässlich und sicher kommunizieren»

Dolphin Systems AG – Ihr starker Partner für Alarmierung, Krisenmanagement und kritische Geschäftskommunikation

Dolphin Systems mit Sitz in Wollerau verfügt über 25 Jahre Erfahrung am Schweizer Markt. Im April 2016 wurde die Dolphin Systems AG Teil der F24 Gruppe.

F24 ist der führende Software-as-a-Service Anbieter für Alarmierung und Krisenmanagement (FACT24) sowie für sensible und kritische Kommunikation (eCall) in Europa. Mit FACT24 bietet F24 eine hochinnovative Lösung und unterstützt weltweit Kunden beim effizienten und erfolgreichen Managen von Incidents, Not- und Krisenfällen. Als erster und einziger nicht-amerikanischer Anbieter ist die F24 AG im aktuellen Gartner Bericht für Notfall-/ Massenbenachrichtigungsdienste (engl.: EMNS) gelistet.

Mit seinem Hauptsitz in München unterliegt das Unternehmen den deutschen Datenschutz-Richtlinien und hostet sein FACT24- SaaS-System ausschliesslich in deutschen Rechenzentren. F24 ist gemäss den internationalen Standards ISO/IEC 27001:2003, ISO 22301:2012 zertifiziert.

Darüber hinaus sorgt F24 durch verschiedene, weitere Massnahmen für zusätzlichen Schutz – für nationale und internationale FACT24-Kunden gleichermassen. Mit der Wahl von FACT24 sind Unternehmen in jeglicher Hinsicht auf Bedrohungslagen optimal vorbereitet, Datenschutz und -Sicherheit natürlich inbegriffen. Darüber hinaus bietet die eCall-Plattform Lösungen für die hochvolumige Kommunikation von kritischen bis vertraulichen Inhalten im Unternehmensumfeld.

Für weitere Informationen kontaktieren Sie uns telefonisch oder über unsere Website www.dolphin.ch.

Dolphin Systems AG
8832 Wollerau, Schweiz
Telefon: +41 (0)44 787 30 70
Fax: +41 (0)44 787 30 71
E-Mail: info@dolphin.ch