Cyber-Hilfswerk:

Eine dringende Antwort auf die Herausforderungen des digitalen Zeitalters

Die fortschreitende Digitalisierung unserer Welt bringt unzählige Vorteile mit sich, doch auch die Risiken und Bedrohungen steigen, insbesondere im Bereich der Cybersicherheit. Cyberangriffe und -kriminalität haben in den letzten Jahren massiv zugenommen, was nicht nur große Unternehmen, sondern auch kleine und mittlere Unternehmen (KMU) sowie Privatpersonen stark betrifft. Um diesen Herausforderungen effektiv zu begegnen, entstand die Idee zur Gründung eines Cyber-Hilfswerks in Österreich, Deutschland, der Schweiz und auf internationaler Ebene.

Die Idee hinter dem Cyber-Hilfswerk

Das Konzept eines Cyber-Hilfswerks basiert auf einer einfachen, aber entscheidenden Erkenntnis: In der digitalen Welt benötigen wir Strukturen, die mit klassischen Katastrophenschutzsystemen wie dem Technischen Hilfswerk (THW) in Deutschland vergleichbar sind. Das THW ist seit Jahrzehnten für seine schnelle und effektive Hilfe in Notlagen bekannt, sei es bei Naturkatastrophen oder technischen Krisen. Diese erprobte Struktur wird nun in die digitale Sphäre übertragen, um eine ähnliche Reaktionsfähigkeit bei Cyberangriffen zu gewährleisten.

Cyberangriffe sind oft komplex und vielschichtig. Eine rein präventive Abwehr reicht in vielen Fällen nicht aus. Es muss sichergestellt werden, dass im Krisenfall Notfallressourcen und schnelle Unterstützung bereitgestellt werden können. Genau hier setzt das Cyber-Hilfswerk an. Es nutzt das Wissen und die Einsatzbereitschaft der Zivilgesellschaft, um technische und personelle Unterstützung im Fall eines Cyberangriffs zu leisten. Besonders KMUs, die oft nicht über die Ressourcen großer Konzerne verfügen, sollen von dieser Struktur profitieren.

Der Zweck des neu gegründeten Vereins

Das Hauptziel des Cyber-Hilfswerks ist klar definiert: Es soll technische und organisatorische Hilfe bei Cyberangriffen bieten. Zu den Aufgaben gehören die Abwehr von Angriffen, die Wiederherstellung von IT-Systemen nach einem Angriff sowie die Prävention durch gezielte Schulungen und Informationskampagnen. Das Cyber-Hilfswerk fungiert somit als eine Art "digitale Feuerwehr", die bei einem Notfall schnell eingreifen kann, um weiteren Schaden abzuwenden.

Die zentralen Aufgaben des Cyber-Hilfswerks sind:

1. **Notfallunterstützung/Notfallhilfe vor Ort:** Im Krisenfall werden qualifizierte IT-Fachleute mobilisiert, die betroffene Unternehmen oder Privatpersonen bei der Krisenbewältigung unterstützen.
   Diese Experten helfen bei der Wiederherstellung der betroffenen Systeme und beraten über zukünftige Sicherheitsmaßnahmen.
2. **Schulungen und Weiterbildung:** Durch Aus- und Weiterbildungen im Bereich Cybersicherheit sollen Bürger und Unternehmen auf mögliche Gefahren vorbereitet werden. Auch die Weiterbildung von Fachpersonal aus KMU und Behörden gehört zu den Aufgaben des Hilfswerks.
3. **Durchführung von Digitalisierungs- und Cyber-Projekten wie z.B. das Projekt CYBER-KIDS (Junior Digital Angels).** Das Cyber-Hilfswerk will 3-jährigen bis 10-jährigen Kindern die Thematik „Digitalisierung und ihre Anwendung“ näherbringen und dabei den richtigen Umgang damit schulen.

Organisation des Cyber-Hilfswerks

Das Cyber-Hilfswerk orientiert sich an den Strukturen klassischer Hilfsorganisationen wie dem Technischen Hilfswerk, dem Roten Kreuz oder eines Automobilclubs, wie z.B. dem ÖAMTC, ADAC oder TCS. Es gibt lokale, regionale und zentrale Standorte in verschiedenen Ländern und durch den Einsatz moderner digitaler Technologien kann das Hilfswerk flexibel und ortsunabhängig agieren. Dies ermöglicht es Fachkräften, remote zu arbeiten und bei Bedarf schnell aktiviert zu werden, um technische Unterstützung zu leisten.

Als Verein strukturiert, ist das Hilfswerk offen für IT-Fachleute und technisch versierte Laien, die sich engagieren und einen Beitrag zur Cybersicherheit leisten möchten. Freiwillige werden regelmäßig geschult und trainiert, um im Ernstfall sofort einsatzbereit zu sein. Die dezentrale Organisation ermöglicht eine flexible Reaktion auf Krisen, ein Vorteil, den herkömmliche Gefahrenabwehrsysteme oft nicht bieten können.

Vorteile für KMU und Privatpersonen

Insbesondere für KMU sowie Privatpersonen bietet das Cyber-Hilfswerk immense Vorteile. Viele kleine und mittlere Unternehmen verfügen nicht über die finanziellen und personellen Ressourcen, um sich gegen komplexe Cyberbedrohungen zu schützen. Ein Cyberangriff kann zu erheblichen finanziellen Verlusten und sogar existenzbedrohenden Produktionsausfällen führen. Das Cyber-Hilfswerk bietet diesen Unternehmen dringend benötigte Unterstützung.

1. **Schnelle Hilfe im Notfall und Krisenfall:** Bei einem Cyberangriff können KMU auf die Hilfe von qualifizierten Fachleuten zurückgreifen, die entweder vor Ort oder remote unterstützen. Dies kann von der Wiederherstellung von Systemen bis hin zur Beratung über zukünftige Sicherheitsmaßnahmen reichen.
2. **Prävention durch Schulungen:** Unternehmen können ihre Mitarbeitenden im Bereich Cybersicherheit weiterbilden, um zukünftige Risiken zu minimieren. Das Identifizieren von Sicherheitslücken und das Umsetzen von präventiven Maßnahmen stehen hierbei im Vordergrund.
3. **Sensibilisierung von Privatpersonen:** Auch Privatpersonen profitieren von den Schulungsangeboten und der Notfallhilfe des Cyber-Hilfswerks. Ein besonderer Fokus liegt dabei auf dem Schutz persönlicher Daten und der sicheren Nutzung digitaler Dienste.

Internationale Dimension und Zusammenarbeit

Die Gründung des Cyber-Hilfswerks ist nicht auf nationale Grenzen beschränkt. In einer global vernetzten Welt ist internationale Zusammenarbeit essenziell. Durch den Austausch von Wissen und Ressourcen können Bedrohungen besser erkannt und gemeinsam abgewehrt werden. Das internationale Cyber-Hilfswerk arbeitet eng mit internationalen Partnern und Organisationen zusammen, um globale Standards im Bereich Cybersicherheit zu fördern und zu etablieren.

Die Rolle der GDCIM - Genossenschaft für Digitalisierung, Challenge und Innovationsmanagement

Parallel zur Gründung des Cyber-Hilfswerks wurde die **GDCIM - Genossenschaft für Digitalisierung, Challenge und Innovationsmanagement** ins Leben gerufen. Diese im Dezember 2022 in Volketswil, Schweiz, gegründete Genossenschaft hat sich zum Ziel gesetzt, kleine und mittlere Unternehmen in der D-A-CH-Region (Deutschland, Österreich, Schweiz) bei der digitalen Transformation zu unterstützen.

Die GDCIM bietet eine Einkaufs- und Leistungsgemeinschaft für spezifische Software- und Hardwarelösungen, die auf die Bedürfnisse von KMU zugeschnitten sind.
Ihr Hauptziel ist es, den Mitgliedern in den Bereichen Digitalisierung und Cyber-Risikomanagement zu helfen. Durch gemeinsame Selbsthilfe sichert und fördert die GDCIM die wirtschaftlichen Interessen ihrer Mitglieder, bietet strategische Beratung und unterstützt bei Notfallmanagement und IT-Instandhaltung.

Ein großer Vorteil der Mitgliedschaft in der GDCIM liegt in der Bereitstellung von kosteneffizienten IT- und Cyberlösungen sowie im Zugang zu einem Netzwerk von Experten und Fachleuten. Besonders für KMUs, die oft nur begrenzte Ressourcen haben, ist dies eine wertvolle Unterstützung.

FAZIT

Das **Cyber-Hilfswerk** und die **GDCIM-Genossenschaft** sind innovative und dringend benötigte Antworten auf die wachsenden Herausforderungen der digitalen Welt. Durch die Kombination von Prävention, Schulung und Krisenintervention bieten sie Unternehmen und Privatpersonen gleichermaßen effektive Unterstützung. Während das Cyber-Hilfswerk im Ernstfall schnell eingreifen kann, leistet die GDCIM wertvolle Arbeit im Bereich der strategischen Beratung und der IT-Instandhaltung. Gemeinsam sind sie ein entscheidender Schritt, um KMU und Privatpersonen in der digitalen Welt sicherer zu machen und Cyberkriminalität effektiv zu bekämpfen.

Über das ZRK:
Das **ZRK - Zentrum für Risiko- und Krisenmanagement** ist eine führende Institution, die Unternehmen und Organisationen bei der Prävention, Bewältigung und Nachbereitung von Risiken und Krisen unterstützt. Mit maßgeschneiderten Lösungen, Schulungen und Beratungen hilft das ZRK, Risiken frühzeitig zu erkennen und effektive Strategien zur Krisenbewältigung zu entwickeln.

Fotos sowie sämtliche Presseunterlagen stehen nach der Pressekonferenz unter www.zfrk.org zum Download zur Verfügung.

Bei Rückfragen:

Mag. Manfred Oschounig
Zentrum für Risiko- und Krisenmanagement
Strategisches Marketing & PR
Tel.: +43 664 2329090
Mail: manfred.oschounig@zfrk.at