

Bericht über die Erhebung des Cybersecurity-Bewusstseins der Angestellten in steirischen Organisationen in Zeiten von COVID-19.

Die COVID-19-Pandemie hat viele Bereiche unseres Lebens stark verändert und hat zahlreiche neue **Angriffsmöglichkeiten für Cyberkriminelle geschaffen**. Die Folgen eines geringen **Cybersecurity-Bewusstseins** der MitarbeiterInnen können für Organisationen folgeschwer sein. Im Rahmen einer anonymen Online-Umfrage¹, an der **über 200 Angestellte aus mehr als 13 Branchen in der Steiermark** teilnahmen, wurde das derzeitige Cybersecurity-Bewusstsein in der COVID-19-Krise und deren Auswirkungen untersucht.

Die Ergebnisse der Studie zeigen, dass mit durchschnittlich **70% der erzielbaren Punkte**, die Angestellten im Allgemeinen **ein gutes Cybersecurity-Bewusstsein** haben. Für eine weitere Steigerung sollte den Bereichen Internetnutzung und Netzwerksicherheit Aufmerksamkeit gewidmet werden, da sich für diese Bereiche ein niedriges Cybersecurity-Bewusstsein zeigte (57% und 61%). Außerdem sollte eine **Cybersecurity-Kultur** z.B. durch klare Cybersecurity-Richtlinien, Awareness-Schulungen, Cybersecurity-Informationshinweise oder regelmäßige Cybersecurity-Bewusstseinstests etabliert werden.

Steirische Organisationen förderten das Cybersecurity-Bewusstsein während der Pandemie durch Mitteilungen im Intranet und Schulungen über Cybersecurity in Zeiten der Pandemie (**50%**), **E-Mails oder textbasierte Informationsseiten** im Firmen-Intranet wurden von 95% der TeilnehmerInnen aus großen Organisationen und Schulungen (virtuell oder persönlich) wurden von 56% genannt und sind die häufigsten Methoden. Kleine Organisationen nutzten Gruppendiskussionen (85%) und E-Mails oder textbasierte Informationsseiten im Firmen-Intranet (78%) in erheblichem Maße um das Cybersecurity-Bewusstseinslevel in Zeiten von COVID-19 zu steigern. Jüngere ArbeitnehmerInnen verfügen über weniger Bewusstsein in Bezug auf Cybersecurity als ältere ArbeitnehmerInnen. Angestellte mit einem mittleren oder höheren Bildungsgrad (Matura, bzw. Universitäts-/Fachhochschulabschluss) haben ein **signifikant höheres Cybersecurity-Bewusstsein** als diejenigen mit Lehr- oder Pflichtschulabschluss.

Cyberkriminelle versuchen die Pandemie zu nutzen und so haben **50% der Befragten** über Phishing-E-Mails mit Corona-Bezug berichtet. Kleine Organisationen scheinen dabei ein häufiges Ziel für Cyberkriminelle zu sein. **Mehr als 85%** der Angestellten von **kleinen Organisationen** geben an, dass während der Pandemie ein Cyberangriff auf Ihre Organisation stattgefunden hat, bei **großen Organisationen** sind es dagegen nur **50%**.

Mehrere Indikatoren zeigen, dass Organisationen in der Steiermark gut auf die Pandemie vorbereitet waren. **Mehr als 65%** der Angestellten aus großen Organisationen geben an, dass sie die Möglichkeit hatten vom Home-Office vor, und **87%** während der Pandemie zu arbeiten. Etwa **35% der Teilnehmenden** erhielten Informationshinweise in Bezug auf Cybersecurity während der Pandemie. Mehr als **70% der Befragten** gaben an, dass innerhalb von einer Woche alle technischen Voraussetzungen für die Angestellten zur Arbeit im Home-Office geschaffen worden sind.

Univ.-Prof. Dr. Stefan Thalmann ,
stefan.thalmann@uni-graz.at
BANDAS-Center, Universität
Graz

Johannes Zeiringer , MSc
johannes.zeiringer@uni-graz.at
BANDAS-Center, Universität Graz.

Haris Alic, Dipl.-Oec
alic.haris@edu.uni-graz.at
Universität Graz

¹ Die Umfrage wurde von Haris Alic in Rahmen der Masterarbeit: "Cybersecurity - Awareness Level and applied Instruments in Styrian organizations" durchgeführt. Das BANDAS-Center in Graz betreute und begleitete die Masterarbeit.