CYBERSICHERHEIT ALS CHANCE

Cyberkriminalität und ihre Prävention bei kleinen und mittleren Unternehmen in Österreich

In Österreich steigt die Zahl der Straftaten im Internet seit Jahren rasant an. Auch für Wirtschaftsunternehmen bedeutet dieses wachsende Kriminalitätsfeld eine neue Herausforderung. Österreichs Unternehmensstruktur ist stark durch KMU (kleine und mittlere Unternehmen) geprägt, über 99 Prozent der österreichischen Unternehmen werden als solche definiert. Es ist daher davon auszugehen, dass diese Unternehmen auch vielfältige Erfahrungen mit Cyberkriminalität gemacht haben.

ZIEL DER STUDIE

Das KFV hat sich mit der hier vorliegenden Studie zum Ziel gesetzt, das Feld der Cyberkriminalität genauer zu durchleuchten.

Die Studie wurde durchgeführt um

> den momentanen Gefährdungs- und Schadensstand wiederzugeben
> eine Einschätzung über zukünftige Trends zu geben sowie
> Tipps zur Vermeidung von Viktimisierung zu geben.

Sie soll als Basis dienen, um den Zustand der Cybersicherheit bei KMU in Österreich darzustellen, Trends, Schwächen und Stärken der betreffenden Prozesse und Strukturen der Unternehmen aufzuzeigen sowie einen Überblick über Maßnahmen zur Prävention von Cyberangriffen zu geben. Gleichzeitig soll sie für Unternehmen als Informationsquelle dienen, die sie für eine Optimierung der eigenen Cybersicherheit nutzen können.

SCHADEN

Einen finanziellen Verlust durch Cyberkriminalität erlitten im Jahr 2019 lediglich 7% der befragten Unternehmen, was fast eine Halbierung im Vergleich zum Jahr 2018 bedeutet (12%).

Der finanzielle Schaden betrug zwischen EUR 130 und 150.000, wobei viele Unternehmen hierzu keine Angaben machen wollten oder konnten.

DIE HAUPTGEFAHREN

Die Hauptgefahren für kleine und mittlere Unternehmen in Österreich im Bereich Cyberkriminalität entstehen durch Ransomware und Phishing.

Über drei Viertel der befragten Unternehmen haben 2019 bereits Phishing-Versuche in ihrem Unternehmen erlebt, und mehr als die Hälfte sah sich bereits mit Schadsoftware konfrontiert. Mit Blick auf die tatsächlich eingetretenen Fälle von Cyberkriminalität dominieren ebenfalls Phishing und Schadsoftware, mit jeweils ungefähr 25% „Erfolgsquote“. Hier gab es im Vergleich zu 2018 bedauerlicherweise auch keine Entspannung. Die eingetretenen Fälle von Phishing verdoppelten sich sogar.

RISIKOBEWUSSTSEIN GERING

In der quantitativen Befragung zeigt sich ebenso, dass die Bedrohung, die von Cyberkriminalität ausgeht, von den Unternehmen selbst tendenziell eher gering eingeschätzt wird, vor allem im Bereich Datendiebstahl.

METHODIK

Im Auftrag des KFV wurde österreichweit eine Online-Representativbefragung, ergänzt durch Tiefeninterviews durchgeführt.

Stichprobe: 500 österreichische kleine und mittlere Unternehmen

Studienzeitraum: September/Oktober 2019

Cyberkriminalität bei kleinen und mittleren Unternehmen

Ergriffene Maßnahmen in Bezug auf Datendiebstahl

25%

Ca. 25 % der Befragten haben Anzeige gegen Datendiebstahl in Bezug auf Kundendaten oder Unternehmensdaten bzw. Passwörter erstattet. Bei Phishing-Versuchen waren das nur 7%.

50%

Ca. 50 % der Befragten haben in Bezug auf Datendiebstahl die Hilfe von einem externen IT-Experten in Anspruch genommen. In Bezug auf Server-Angriffe waren es fast 90%.

50%

Über 50 % der Befragten konnten die Situation beim Datendiebstahl ohne externe Hilfe lösen. Im Bereich Ransomware waren es ca 40%. Bei Phishing-Versuchen haben weitere 9% nichts unternommen.

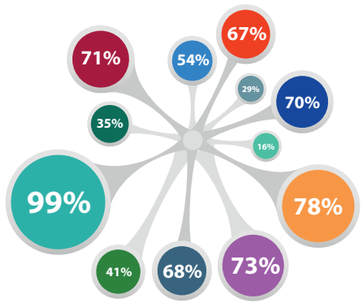
Versuchte Formen von Cyberkriminalität

77% der KMU haben Phishing-Versuche erlebt

51% haben Angriffsversuche durch Schadsoftware oder Ransomware erlebt

20% andere Formen der Cyberkriminalität

Ergriffene Schutzmaßnahmen



Top 3

99% Anti-Viren-Software, Firewall

78% Beratung durch externe IT-Experten

73% Serverlösungen zum Schutz gegen externe Attacken

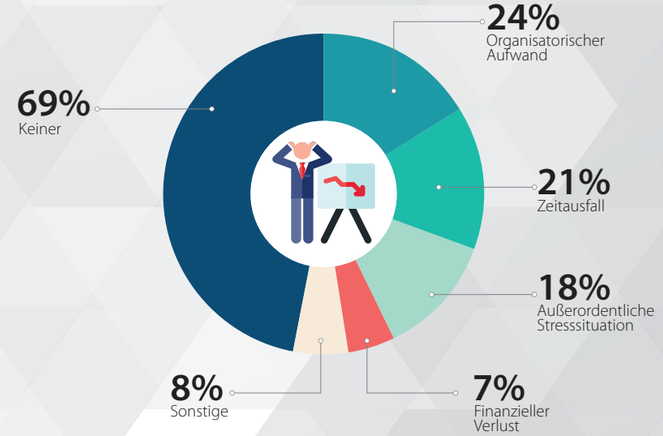
Bottom 3

35% Risikobewertung durch externe Experten

29% Spezielle Sicherheitsprogramme gegen Datendiebstahl

16% Abschluss von Versicherungen gegen dieses Risiko

Erlittener Schaden



RISIKEN

Ransomware ist eine Form von Schadsoftware, in der Daten gekidnappt werden. Die Angreiferin verschlüsselt die Daten der Opfer und verlangt ein Lösegeld, um das Passwort zu erhalten. Ransomware kann über E-Mail-Anhänge, infizierte Programme oder kompromittierte Webseiten verteilt werden.

Phishing beschreibt den Versuch des Diebstahls von Kennungen und Passwörtern per Internet durch den Versand von gefälschten E-Mails oder SMS. Internet-Anwender werden von Cyberkriminellen mittels täuschend echt nachgemachter E-Mails auf gefälschte Internetseiten von Banken, Onlineshops oder anderen Onlinediensten gelockt um dort deren Benutzerkennungen und Passwörter zu ergattern.

Bei einem **DDoS-Angriff** führen Angreifer die Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbei. Einer der Wege ist das Infizieren von mehreren Rechnern mit Schadsoftware, mit der sie unbemerkt die Kontrolle über diese Computer übernehmen. Die Angreifer missbrauchen dieses infizierte Rechner-Netz, auch Botnetz genannt, ferngesteuert für ihre DDoS-Attacken. Mit dem Botnetz greifen sie parallel ihr Ziel an und beschießen dabei dessen Infrastruktur mit zahllosen Anfragen.

Beim **Datendiebstahl** verschaffen sich Unbefugte geheime, geschützte oder nicht für sie vorgesehen Daten wie personenbezogene Daten. Die Daten lassen sich anschließend missbräuchlich verwenden. Der Datendiebstahl kann sich auf digital gespeicherte oder auf physischen Medien wie Papier abgelegte Daten beziehen. Rahmenwerk für die klare, reibungslose und effiziente Schnittstelle zwischen bemannter und unbemannter Luftfahrt, Dienstleister und Behörden.

GEFAHREN & ERFAHRUNGEN

- 60% der (weltweit) betroffenen Unternehmen sind KMU.
- Knapp 80% der österreichischen KMU haben schon Versuche erlebt.
- Die Größte Gefahr ist Phishing (Verdoppelung im Vergleich zu 2018).

DSGVO BEACHTEN!

- Melde- und Benachrichtigungspflichten an die Datenschutzbehörde.
- Geldbußen von bis zu EUR 10 Mio. oder bis zu 2 % des gesamten Jahresumsatzes.
- Nur jeder vierte Betrieb hält die Meldepflicht ein.

Quelle: KFV (Kuratorium für Verkehrssicherheit)

www.kfv.at

PRÄVENTIONSTIPPS

> Für **Passwortsicherheit** sorgen: Gerade kleine Unternehmen können bereits durch eine ausgereifte Passwort-Politik ein Mehr an Sicherheit schaffen. Das bedeutet, dass es eine regelmäßig durchgeführte Änderung aller relevanten Passwörter gibt, dass betriebsfremde Personen keine Passwörter erhalten und dass die Passwörter nach bestimmten Kriterien gewählt werden.

> Regelmäßig **Updates** durchführen: Hier sehen die Experten am meisten schnelles und einfaches Verbesserungspotential. Regelmäßige Updates des Betriebssystems, von Schutzsoftware, aber auch von kleinen Elementen die Software beinhalten (wie Router, Produktionsmaschinen usw.) können Sicherheitslücken schließen und somit unerlaubtes Eindringen in die IT-Infrastruktur zumindest massiv erschweren.

> Sich um einen guten **Basisschutz** kümmern: Dieser Basisschutz besteht aus einem Antivirusprogramm, einer Scansoftware sowie im Idealfall einem externen Sicherheitsmonitoring. Hier können Unternehmen entweder von spezialisierten Unternehmen für ihre jeweiligen Anforderungen maßgeschneiderte Lösungen zukaufen, oder auf sehr gute fertige Produktlösungen und Pakete für einen ganzheitlichen IT-Security Ansatz zugreifen.

> Ein weiterer zentraler Punkt ist, dass für die zentralen Datensätze, Datenbanken und Systeme **regelmäßige Backups** erstellt werden. Diese Vorkehrungsmaßnahme sorgt dafür, dass selbst bei einem erfolgreichen Angriff der Schaden für das Unternehmen möglichst gering gehalten wird, da der Status Quo ante zügig wieder hergestellt werden kann.

> Eine **Verschlüsselung der Datenträger und Datensysteme** kann ebenfalls dazu beitragen, die Datensicherheit zu optimieren.

> **IT-Sicherheitsbeauftragten schulen und ausbilden lassen.** Hier bietet sich zum Beispiel der Lehrgang „Certified Data & IT Security Expert“ der WKO an. Darüber hinaus werden auch regelmäßige Schulungen der Belegschaft/der zuständigen Personen als wichtiger Aspekt einer umfassenden Prävention herausgestellt.

IM **NOTFALL**

MELDESTELLEN

24h Meldestelle des C4 im BMI:
T: + 43-(0)1 24836 986500
E: against-cybercrime(at)bmi.gv.at

Anzeigen können auch an jeder **Polizeidienststelle** erstattet werden.

WKO

24h Cyber-Security-Hotline
T: 0800 888 133

Die WKO bietet für Mitglieder die **Cyber-Security-Hotline**, die rund um die Uhr erreichbar ist.

NÜTZLICHE LINKS

www.nomoreransom.org

id-ransomware.malwarehunterteam.com

Quelle: KFV-Studie zur Cyberkriminalität bei KMU
Gallup-Institut im Auftrag des KFV

Medieninhaber und Herausgeber:
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18, A-1100 Wien
Tel: +43-(0)5 77 0 77-0
E-Mail: kfv@kfv.at