Datum: 04.02.2021

ORGANISATOR
DAS MAGAZIN FÜR KMU

Der Organisator
9230 Flawil
058 / 344 97 37
https://www.organisator.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'801
Erscheinungsweise: 10x jährlich

Seite: 35
Fläche: 126'553 mm²

Auftrag: 3013971
Themen-Nr.: 663.038

Referenz: 79697003
Ausschnitt Seite: 1/3

«IT-Security ist Basishygiene – wie Zähneputzen»

Cybersicherheit betrifft uns alle – mehr denn je. Denn die Digitalisierung schreitet fort, befeuert durch die Folgen der Corona-Pandemie sogar noch schneller als zuvor. Und mit noch mehr Homeoffices wächst die Angriffsfläche für Cyberkriminelle exponentiell. Davor warnen Experten wie Nicolas Mayencourt.

VON THOMAS BERNER

Hacker sind heute keine Nerds im Kapuzenpulli mehr, die nächtelang vor ihren PCs sitzen und versuchen, Passwörter zu knacken. «Cybercrime ist ein lukratives Business geworden, geführt durch professionell geführte Organisationen, deren Chefs in Anzug und Krawatte auftreten», sagt Nicolas Mayencourt. Er weiss, wovon er spricht. Als Gründer und CEO von Dreamlab Technologies berät er Firmen und Behörden bei der Abwehr und Prävention von Cyberangriffen. Er, der selbst einmal als Hacker angefangen hat, liefert eindrückliche Zahlen: «2019 haben die zehn grössten Internetfirmen insgesamt 700 Billionen US-Dollar umgesetzt. Der Umsatz im Rauschgifthandel betrug im selben Jahr 1,2 Trillionen US-Dollar. Und mit Cybercrime wurden geschätzte 1,5 Trillionen US-Dollar umgesetzt!». Das heisst: Der Handel mit illegalen Gütern und Dienstleistungen hat inzwischen ein Volumen angenommen, das unser Vorstellungsvermögen übersteigt. Der Schluss, den Nicolas Mayencourt daraus zieht: «Cybercrime ist hochrelevant und geht uns alle an.»

ORGANISATOR **Herr Mayencourt, in letzter Zeit wurden diverse Fälle von Cyberkriminalität bei Grossunternehmen (z.B. Huber+Suhner, TX Group) wie auch bei KMU publik. Was läuft bzw. lief bei diesen Unternehmen falsch?**

NICOLAS MAYENCOURT Vieles... Dahinter steht letztlich ein Mix von Nachlässigkeit bei der Sicherheit und dem Fortschritt der Cyberkriminellen. Diese werden immer geschickter und besser. So machen sie sich etwa das wegen Corona erhöhte Informationsbedürfnis zunutze und verschicken Fake-Nachrichten, z.B. getarnt als Mitteilung des BAG. Und da kann ein Klick schnell mal einer zu viel sein.

Wie ist es um die Cybersicherheit von KMU in der Schweiz bestellt? Stellen Sie einen Lerneffekt aufgrund der eingangs erwähnten Fälle fest?
Ja. Unsere Gesellschaft ist dabei, aufzuwachen. Denn wir müssen aufhören, naiv zu sein. Wir sind mehr denn je abhängig von der Technologie. Deshalb muss massiv in die Sicherheit investiert werden. Und das wird endlich getan. Andernfalls laufen wir Gefahr, dass einmal alles zusammenbricht.

Aber trotzdem ist man immer noch im Rückstand?
Absolut, denn warnende Stimmen gab es ja schon lange. Ich ziehe da einen Vergleich zum Klimawandel. Den hat der Club of Rome bereits in den 1960er-Jahren prophezeit. Aber erst jetzt, wo es allmählich wehtut, beginnt man zu handeln. Die Beispiele, die Sie zu Beginn erwähnt haben, zeigen einen Wandel hin zu einer positiven Fehlerkultur. Fehler zu machen war lange Zeit ein Tabu. Aber es ist notwendig, aus Fehlern zu lernen. Deshalb sprechen etwa an den Swiss Cyber Security Days Firmen explizit über ihre Erfahrungen mit Cyber-

IT-Sicherheit für KMU

Die IT-Sicherheitsexperten Nicolas Mayencourt und Marc K. Peter helfen mit ihrem neuen Buch «IT-Sicherheit für KMU» KMU-Inhabern dabei, wichtige Vorkehrungen zu treffen, sich selbst, ihre Mitarbeitenden und Partner zu sensibilisieren und mit IT-Fachkräften weitere Sicherheitsvorkehrungen zu planen. Die Lesenden erfahren zudem, welche Strategien sich bewährt haben, um sich gegen Bedrohungen und Risiken durch Technologien, das Internet und die Digitalisierung zu schützen. Das Buch (ISBN 978-3-03875-343-8) ist im Beobachter-Verlag erschienen und auch dort erhältlich.

>shop.beobachter.ch

Das Thema IT-Sicherheit für KMU wird am 10. und 11. März an den Swiss Cyber Security Days, welche virtuell stattfinden, speziell beleuchtet. Nicolas Mayencourt wird dort als Referent zu diversen Herausforderungen Stellung nehmen.

Datum: 04.02.2021

ORGANISATOR
DAS MAGAZIN FÜR KMU

Der Organisator
9230 Flawil
058 / 344 97 37
https://www.organisator.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'801
Erscheinungsweise: 10x jährlich

Seite: 35
Fläche: 126'553 mm²

Auftrag: 3013971
Themen-Nr.: 663.038

Referenz: 79697003
Ausschnitt Seite: 2/3

kriminalität. Die Lehren, die sie daraus gezogen haben, wollen sie anderen Unternehmen weitergeben. Denn erfolgreiche Cyberangriffe haben schon ganze Firmen in den Konkurs getrieben.

Wo lauern denn die grössten Gefahren? Wie gross ist etwa der Anteil an KMU, die auf ihren Computern noch veraltete Software benutzen?
Da geht es nicht nur um KMU, sondern häufig leider auch um systemkritische Industrien, wie etwa die Gesundheits- oder Stromversorgung. Da sind noch viel zu oft veraltete Systeme im Einsatz. Solange diese isoliert und ohne Remote-Zugriff laufen, mag dies ja noch angehen. Doch bekanntlich wird alles immer mehr vernetzt. Der Hintergrund dieser – aus meiner Sicht gefährlichen – Situation liegt vielfach in zu starren Regulatorien. Denn viele Geräte unterliegen Typenprüfungen. Immer wenn etwas geändert werden muss, und sei es nur die Steuerungssoftware, dann muss das Gerät ein erneutes Zulassungsverfahren durchlaufen. Dies ist teuer, und naturgemäss scheut man da die Kosten – leider zuungunsten der Sicherheit.

Wie verschärft sich die Situation durch die Homeoffice-Pflicht?
Die Auswirkungen der Corona-Pandemie zwang viele Unternehmen zu einer schnellen Digitalisierung. Dies erfolgte nicht überall gleich ordentlich, Sicherheitsbedenken kommen da oft zu kurz. Schauen Sie: Bisher bildete die IT-Infrastruktur eines Unternehmens eine einzige, überschaubare Unit. Indem Firmen nun ihre Mitarbeitenden in ihre Homeoffices schicken, kommt eine Vielzahl kleiner Units hinzu, entsprechend hat sich der Perimeter und damit die Angriffsfläche eines Unternehmens explosionsartig erweitert. Denn die einzelnen Homeoffices sind oft nicht genügend gesichert, die dortige IT-Infrastruktur wird zudem mit Mitbewohnern – Lebenspartner, Kinder – geteilt. Da können sich analog dem Coronavirus auch Computerviren sehr leicht verbreiten. Mich erstaunt eigentlich, wie wenig Schaden aufgrund dieser Risikosituation bisher angerichtet wurde.

Worauf sollten Unternehmen in Sachen IT-Sicherheit bei ihren Mitarbeitenden im Homeoffice besonders Wert legen? Empfiehlt sich z.B. ein «Approval» von privaten Geräten durch den Cyberverantwortlichen eines Unternehmens?
Wenn ein Unternehmen seinen Mitarbeitenden zentral gemanagte Geräte zur Verfügung stellt, ist das gewiss ein guter Ansatz. Die Idee einer Inspektion von privaten Geräten mag gut klingen, ist in der Praxis aber nicht umsetzbar. In der Konsequenz müsste dies über eine totale Überwachung gehen, und das will niemand.

Und nicht zuletzt ist da noch der Mensch ein Unsicherheitsfaktor?
Da muss ich Ihnen widersprechen! Gerade der Mensch kann das stärkste Glied in der Sicherheitskette sein. Entsprechend müssen Massnahmen genau da ansetzen: Den Menschen nicht als Risiko, sondern als Chance betrachten. Und das kann nur über kontinuierliche Schulung und Sensibilisierung gehen. Viele wirtschaftliche Schäden sind nicht technischer Natur; wenn aber nur einem Mitarbeitenden ein E-Mail, das nach CEO-Fraud aussieht, auffällt, dann wird der Mensch zum besten Alarmsystem.

«Cyberangriffe haben schon ganze Firmen in den Konkurs getrieben»

Im Januar wird ein Buch von Ihnen veröffentlicht (beim Beobachter-Verlag?). Was hat Sie dazu inspiriert?
Die KMU sind nicht nur auf dem Papier das Rückgrat der Schweizer Wirtschaft. Im Verhältnis zu ihrer Anzahl ist es um ihre Sicherheitskultur nicht gut genug bestellt. Die wenigsten haben eine eigene IT Security Unit. Und eine Sensibilisierung bezüglich Cybersicherheit ist auf allen Ebenen – Verwaltungsrat, Management, Mitarbeitende – kaum vorhanden. Mit unserem Buch wollen wir deshalb einen Praxisratgeber bieten mit Checklisten und Sicherheitsleitfäden. Diese zeigen wir anhand von drei repräsentativen «Modell-KMU»: einem Coiffeur-Salon, einem Detailhändler und einem Ingenieurbüro mit verschiedenen Standorten. Damit wollen wir Betroffenheit wecken. Wir zeigen: Vieles bei der IT-Security ist Basishygiene – wie Zähneputzen. Dazu gehören Fragen wie z.B.: Gibt es Back-ups? Werden verschiedene Passwörter verwendet? Gibt es Notfallpläne und wurden diese schon mal geübt? Solche Dinge benötigen keine grossen Investitionen.

Welche Empfehlungen geben Sie KMU in Sachen Cybersicherheit?
Achten Sie darauf, dass Geräte nur von einer Person genutzt werden, und checken Sie regelmässig, ob Antivirensysteme aktiv und alle Sicherheits-Patches installiert sind. Dennoch bleiben da immer noch Lücken offen. Ein anderer Weg: Früher wählten sich alle Endgeräte in einen Server ein, sie waren für sich allein also «dumm». Solche Systeme, z.B. Citrix, mit einer virtuellen Desktop-Struktur, sind wieder im

Datum: 04.02.2021

ORGANISATOR
DAS MAGAZIN FÜR KMU

Der Organisator
9230 Flawil
058 / 344 97 37
https://www.organisator.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'801
Erscheinungsweise: 10x jährlich

Seite: 35
Fläche: 126'553 mm²

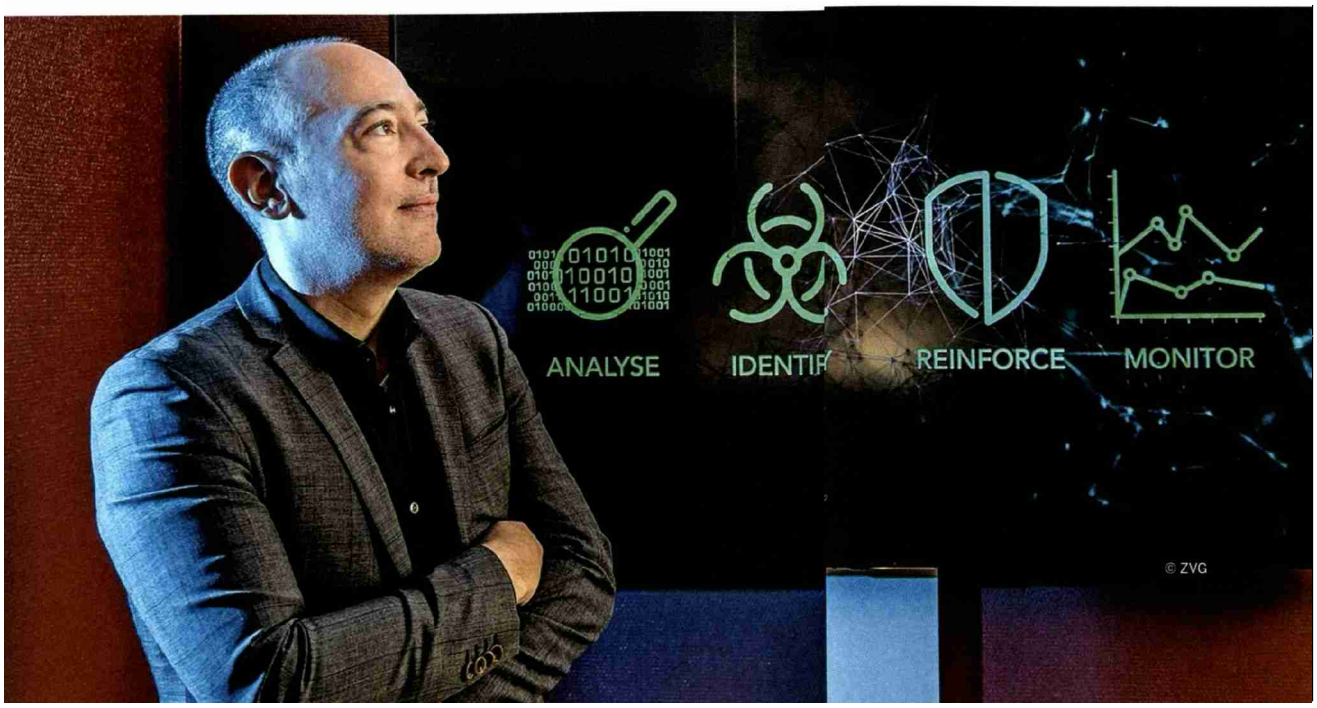
Auftrag: 3013971
Themen-Nr.: 663.038

Referenz: 79697003
Ausschnitt Seite: 3/3

Kommen und ergeben Sinn. Zudem sind sie auch kosteneffizient. Und, wenn Sie mir etwas Schleichwerbung gestatten: Kaufen Sie unser neues Buch.

Was ist von Versicherungen gegen Cyberkriminalität zu halten? Welche Modelle empfehlen Sie da?
Auch hier zunächst ein paar Zahlen, um das Ganze etwas einzuordnen: Der Schaden, der direkt durch Cyberangriffe entstanden ist, wird Ende 2020 weltweit mit 100 Milliarden Franken beziffert. Zum Vergleich: Für die Schweiz spricht der Schweizerische Versicherungsverband von einer Schadensumme von 9,5 Milliarden Franken (Direktschäden). Betreffend Cyberversicherungen bin ich etwas gespalten: Versicherungen sind eine gute Sache, um letztlich nicht abwägbare Risiken abzusichern. Aber: Unternehmen sollten vorher ihre Hausaufgaben machen und sich gegen Cyberrisiken wappnen und gegen das Restrisiko versichern. Denn: Keine Versicherung deckt Reputationsschäden und den effektiven finanziellen Schaden.

Und was bringt die Zukunft?
Der Organisationsgrad der Cyberkriminellen wird weiter wachsen. Zu befürchten ist, dass auch immer mehr staatliche Organe involviert sein können. So könnten etwa Hacker im Auftrag eines Staates einem Unternehmen Daten stehlen, dieses damit erpressen und einen Teil davon veröffentlichen – bevorzugt die weniger wichtigen, während die wertvollen Daten weiterverkauft werden. Entscheidend wird sein, wie sich die «Nicht-Kriminellen» verteidigen werden und so dem Cybercrime weniger Raum geben. Wir haben es also in der Hand, ob die 1,5 Trillionen US-Dollar wachsen oder nicht. Damit beschäftigen wir uns auch an den Swiss Cyber Security Days, die übrigens auch viel Wissenwertes für KMU transportieren.



Nicolas Mayencourt fordert noch mehr Sensibilisierung für Cyberrisiken auf allen Unternehmensebenen.