BYE, BYE HACKER!

Cyberkriminalität ist ein wichtiges Thema! Was sind die größten Risiken und was können Sie tun, um Ihr Unternehmen zu schützen, damit Ihre Mitarbeiter sicher arbeiten können?

Share, inspire, have fun!
With CTOUCH by your side.

CTOUCH®

SICHERES ARBEITEN UND ZUSAMMENKOMMEN IN EINER DIGITALEN WELT

Heutzutage ist alles und jeder „vernetzt". Die technologischen Entwicklungen vollziehen sich in rasantem Tempo und bieten Unternehmen eine Fülle neuer Möglichkeiten. Während der Coronakrise führte Grant Thornton eine weltweite Untersuchung darüber durch, was Unternehmen von der Zeit nach der Krise erwarten. Es ist völlig klar, dass die Digitalisierung und die Investitionen in Technologie deutlich zunehmen werden.

Mit der fortschreitenden Digitalisierung nimmt auch die Cyberkriminalität zu. Jeder, der sich in die digitale Welt begibt, kann Opfer dieser neuen Form der Kriminalität werden, und das gilt auch für Unternehmen. Überlegen Sie einmal, wie viele Computer, Laptops, Tablets und Smartphones in Ihrem Unternehmen verwendet werden. Auf jedem dieser Geräte sind wichtige Informationen gespeichert: von persönlichen Daten bis hin zu vertraulichen Geschäftsinformationen. Wenn diese Geräte Opfer eines Cyberverbrechens wie z. B. eines Hackerangriffs werden, könnten die Daten in die falschen Hände geraten. **Jedes Unternehmen, das gehackt wurde, weiß, was das bedeutet: Es kann Ihrem Image erheblichen Schaden zufügen. Darüber hinaus könnten die Daten Ihrer Kunden nach außen dringen, was unter Umständen hohe Geldstrafen nach sich zieht.**

CTOUCH®

MODERNE, SICHERE ARBEITSPLÄTZE

Die digitale Welt erlaubt uns mittlerweile, überall zu arbeiten: Ob im Büro, auf dem Sofa oder am Strand. Aber wie stellt man sicher, dass die Mitarbeiter an all diesen Orten gleichermaßen sicher arbeiten? Es ist Sache des Arbeitgebers, hier für Sicherheit zu sorgen. Daher sollten Sie sich der Risiken bewusst sein, die Sie als Unternehmen eingehen. Machen Sie die digitale Sicherheit zur Priorität und vermeiden Sie es, ein interessantes Ziel für Cyberkriminelle zu werden.

Wissen Sie, welche Gefahren auf Sie lauern? Und was Sie dagegen tun können? In diesem Whitepaper haben wir die häufigsten Cyber-Bedrohungen und Schwachstellen aufgelistet. Wir geben Ihnen auch einige Tipps, wie Sie Cyberangriffe verhindern, damit Ihre Mitarbeiter sicher arbeiten können.

Vorsicht ist besser als Nachsicht!

DIE HÄUFIGSTEN CYBER-BEDROHUNGEN FÜR UNTERNEHMEN

ACHTEN SIE AUF DIE FOLGENDEN DIGITALEN BEDROHUNGEN

SPYWARE

Spyware ist eine Form von Malware (bösartige Software). Es handelt sich um einen schädlichen Code, der sich unbemerkt im Hintergrund Ihres Systems einnistet und vertrauliche Informationen wie Kennwörter und Kreditkartennummern überträgt.

RANSOMWARE

Ransomware ist eine „Software zur Geiselnahme", die Ihre Dateien in Ihrem Netzwerk verschlüsselt. Im Anschluss wird dann ein Lösegeld gefordert (in der Regel Bitcoins), damit Ihre Dateien wieder zugänglich werden.

PHISHING

Phishing ist ein digitaler Betrug über Links oder Anhänge in E-Mails oder per SMS. Damit erhalten Cyber-Kriminelle Zugriff auf Computer mit (vertraulichen) Daten.

DDOS-ANGRIFF

DDoS steht für Distributed Denial of Service. Dabei wird ein Server wird so massiv angegriffen, dass er langsamer wird oder gar nicht mehr funktioniert. Systeme, Netzwerke oder Websites können dadurch ausfallen.

CEO-BETRUG

Eine Form des Betrugs, bei der versucht wird, Menschen dazu zu bringen, Geld auf das Bankkonto des Betrügers zu überweisen, indem sich der Angreifer als CEO oder eine andere hochrangige Person eines Unternehmens ausgibt.

Share, inspire, have fun!
With CTOUCH by your side.

CTOUCH®

DIE HÄUFIGSTEN SCHWACHSTELLEN FÜR UNTERNEHMEN

WAS SIND DIE SCHWACHSTELLEN IN IHREM UNTERNEHMEN?

LIEFERANTENKETTE

Sie selbst mögen die Sicherheitsangelegenheiten in Ihrem Unternehmen bestmöglich geregelt haben; wenn jedoch ein Lieferant Zugriff auf Ihre IT-Umgebung hat und weniger scharfe Sicherheitsvorkehrungen getroffen hat, kann das trotzdem unangenehme Folgen haben.

VERLUST ODER DIEBSTAHL

Der Verlust oder Diebstahl von Geräten wie Laptops, Telefonen und USB-Sticks stellt ein großes Risiko für die Datensicherheit dar. Damit ist es so, als würden Ihre Daten einfach auf der Straße herumliegen.

BRING YOUR OWN DEVICE

Die Mitarbeiter loggen sich zunehmend mit ihren eigenen Geräten in Unternehmensnetzwerke ein. Die Tatsache, dass diese Geräte in der Regel nur unzureichend verwaltet und gesichert sind, macht es Cyberkriminellen leicht, auf Unternehmensdaten zuzugreifen.

WIEDERVERWENDUNG VON KENNWÖRTERN

Die Wiederverwendung derselben Kennwörter für verschiedene Systeme stellt eine große Gefahr dar. Damit können Cyberkriminelle in jedes System eindringen, in dem dieses Kennwort verwendet wird.

EIGENE MITARBEITER

Wussten Sie, dass 90 % aller Datenschutzverletzungen auf menschliches Versagen zurückzuführen sind? In den meisten Fällen geschieht es nicht absichtlich; oft sind sich die Menschen einfach nicht bewusst, dass sie unsicher arbeiten.

PRAKTISCHE CHECKLISTE ZUM VERMEIDEN VON CYBERANGRIFFEN

Es lässt sich nie ganz ausschließen, dass Sie es einmal mit Cyberkriminalität zu tun haben werden. Sie können jedoch versuchen, das Risiko soweit wie möglich zu begrenzen. Mit den folgenden 8 Tipps arbeiten Ihre Mitarbeiter überall sicher. Wie viele Punkte können Sie abhaken?

- ☐ **Virenschutz-Software verwenden.** Vergewissern Sie sich, dass alle Laptops und anderen Geräte durch Antiviren-Software geschützt sind, um zu verhindern, dass sie versehentlich Malware herunterladen.

- ☐ **Aktualisierungen durchführen.** Die Hersteller von Geräten und Software arbeiten ständig daran, ihre Produkte sicherer zu machen. Prüfen Sie, ob Geräte und Software auf dem neuesten Stand sind und aktivieren Sie automatische Updates.

- ☐ **Sichere Einstellungen wählen.** Standardeinstellungen können bequem sein, aber sie können Ihr Unternehmen auch anfällig für Cyber-Bedrohungen machen. Haben Sie daher ein kritisches Auge auf Funktionen, die automatisch „eingeschaltet" sind.

- ☐ **Zugang einschränken.** Minimieren Sie das Risiko von Unfällen und Missbrauch. Legen Sie für jeden einzelnen Mitarbeiter fest, auf welche Systeme und Daten er oder sie zugreifen muss, um zu arbeiten. Erweiterte Zugriffsrechte sollten nur denjenigen gewährt werden, die sie benötigen.

- ☐ **Eine robuste Online-Umgebung bereitstellen.** Installieren Sie starke Firewalls und Internet-Gateways, um Ihr Netzwerk vor Cyber-Angriffen, unbefugtem Zugriff und bösartigen Inhalten zu schützen.

- ☐ **Dritte gründlich prüfen.** Vergewissern Sie sich, dass bei allen externen Plattformanbietern, Lieferanten und anderen Dritten, mit denen Sie zusammenarbeiten, die digitale Sicherheit an erster Stelle steht.

- ☐ **Systeme kontinuierlich überwachen.** Ein Hacker hört nicht auf zu arbeiten, wenn Ihr Arbeitstag endet, das Wochenende beginnt oder Sie in Urlaub fahren. Stellen Sie sicher, dass Sie alle Ihre Systeme kontinuierlich auf ungewöhnliche Aktivitäten, die auf einen Angriff hindeuten könnten, überprüfen und analysieren.

- ☐ **Mitarbeiter zum sicheren Verhalten anregen.** Sensibilisieren Sie Ihre Mitarbeiter und organisieren Sie regelmäßige Informationsveranstaltungen zu den neuesten Cyber-Bedrohungen und Trends. Mindestens ebenso wichtig wie die Technik ist die Schulung und Ausbildung Ihrer Mitarbeiter.

SICHERES ARBEITEN IN KONFERENZRÄUMEN

Während Engagement, Spaß und menschliche Interaktion unsere Leidenschaft sind, nehmen wir Daten- und Cybersicherheit sehr ernst, von Unternehmensdaten bis hin zum Schutz der Privatsphäre. Sicherheit ist nicht umsonst einer der vier Grundwerte des CTOUCH Circle.

Eine gute Sicherheitsgrundlage ist die Basis für eine gesunde und erfolgreiche Organisation. Deshalb setzen wir alles daran, Lösungen und Dienstleistungen zu entwickeln, bei denen die Sicherheit im Vordergrund steht. Unsere Produkte sind so konzipiert, dass die Risiken eines unerwünschten Zugriffs jetzt und in Zukunft minimiert werden.

Sind Sie neugierig, wie wir die Sicherheit auch in Ihren Konferenzräumen gewährleisten können? Unsere Experten helfen Ihnen gerne weiter.

Zeit für eine Revolution der sicheren Meetings!

Unsere Sicherheitspartner

Grant Thornton

CYBER RESILIENCE CENTER BRAINPORT
for the high-tech industry in The Netherlan

CTOUCH®

Hallo, wir sind CTOUCH

CTOUCH hilft Unternehmen dabei, eine sichere, moderne Arbeitsplatz zu schaffen, an dem ihre Mitarbeiter effizienter zusammenarbeiten können. Wir fördern Interaktivität, Produktivität und Engagement bei Meetings, Workshops, Versammlungen – überall. Wie wir das machen? Durch Nutzen der unendlichen Möglichkeiten des Touchscreens! Zur Inspiration. Um Wissen zu teilen. Eigentlich für alles! Deshalb unterstützen wir Sie in jeder Umgebung, in der Sie die Zusammenarbeit fördern wollen oder müssen. Wir kümmern uns darum! Und wir werden Sie verblüffen. Versprochen!

Zögern Sie nicht, uns zu kontaktieren über:

+ 49 (0)211 240 9139 of info@ctouch.eu

www.ctouch.eu/de/security

Share, inspire, have fun!
With CTOUCH by your side.

1726V21111o DE