In einer Welt, die zunehmend digital vernetzt ist, wird Cybersicherheit nicht nur zu einer technischen Notwendigkeit, sondern zu einem grundlegenden Pfeiler des Schutzes unserer persönlichen Daten, der Integrität von Unternehmen und der nationalen Sicherheit.

Zuerst ein paar Zahlen

Wir haben uns dazu entschieden, dieses Thema mehr in den Fokus zu nehmen, als wir auf folgende Zahlen vom BSI (Bundesamt für Sicherheit in der Informationstechnik), Bitkom und HDI aufmerksam geworden sind:

206.000.000.000 Euro Schaden durch **Cyberkriminalität** pro Jahr
95.000 Euro durchschnittliche **Schadenssumme** erfolgreicher Angriffe bei kleinen und mittleren Betrieben
250.000 neue **Schadprogramm-Varianten** werden durchschnittlich **täglich** gefunden
2.000 Schwachstellen in **Softwareprodukten** werden durchschnittlich im **Monat** bekannt
66% aller Spam **Mails** sind **Cyberangriffe**

Die Zahlen zeigen, dass man sich mit dem Thema befassen muss. Wegignorieren hilft da leider gar nicht.

Zuerst ein paar Begriffsbestimmungen

1. Der Bereich der Cybersicherheit umfasst viele verschiedene Arten von Bedrohungen, die sich in ihrer Funktionsweise, ihren Zielen und den Methoden ihrer Verbreitung unterscheiden. Ich werde hier eine einfache Erklärung für jede der genannten Kategorien geben:
2. Phishing: Bezieht sich auf betrügerische Versuche, meist per E-Mail, Telefonanruf oder Textnachricht, bei denen sich Kriminelle als eine vertrauenswürdige Quelle ausgeben, um sensible Informationen wie Benutzernamen, Passwörter oder Kreditkartennummern zu erlangen. Das Ziel ist oft, Zugang zu persönlichen oder Unternehmenskonten zu erlangen oder direkt finanziellen Betrug zu begehen.
3. Malware: Ein Überbegriff, der jegliche Art von schädlicher Software umfasst, die entwickelt wurde, um einem Computer oder Netzwerk Schaden zuzufügen oder unbefugten Zugriff darauf zu erlangen. Viren, Würmer, Trojaner und Ransomware fallen alle unter diese Kategorie.
4. DDoS (Distributed Denial of Service): Eine Attacke, die darauf abzielt, einen Online-Dienst, eine Website oder ein Netzwerk unzugänglich zu machen, indem es mit einer überwältigenden Menge von Datenverkehr aus vielen verschiedenen Quellen überflutet wird. Ziel ist es, die normalen Operationen zu stören oder lahmzulegen.
5. Viren: Eine Art von Malware, die sich selbst replizieren und verbreiten kann, indem sie sich an andere Programme oder Dokumente anhängt. Sobald sie aktiviert ist, kann sie Schaden anrichten, Daten löschen oder andere schädliche Aktionen ausführen.
6. Ransomware: Eine spezifische Art von Malware, die Daten auf dem betroffenen System verschlüsselt oder den Zugriff darauf sperrt und von den Opfern ein Lösegeld für die Entschlüsselung oder Freigabe ihrer Daten fordert.
7. Trojaner: Eine Art von Malware, die sich als legitime Software tarnt. Sobald sie aktiviert ist, kann sie dem Angreifer ermöglichen, Zugang zum infizierten System zu erlangen und dieses zu kontrollieren, oft ohne das Wissen des Benutzers.
8. Keylogger: Eine spezifische Art von Malware oder Überwachungssoftware, die darauf

ausgelegt ist, die Tastenanschläge auf einer Tastatur zu erfassen und zu speichern. Dies kann dazu verwendet werden, Passwörter, persönliche Informationen oder andere sensible Daten zu stehlen.

9. Diese Bedrohungen können erhebliche Schäden anrichten und erfordern unterschiedliche Präventions- und Reaktionsstrategien, um sie effektiv zu bekämpfen

Es gibt viel Hilfe, nicht nur für den Handel

Dankenswerterweise gibt es aber viel Unterstützung seitens der Bundesregierung, die sich des Themas angenommen hat:

Das BSI stellt unter diesem LINK ein großes Paket an Informationen und Empfehlungen zusammen
Die Transferstelle Cybersichereit stellt unter diesem LINK konkrete Präventions- und Hilfsmaßnahmen zur Verfügung
Händler in NRW bekommen von der Landesregierung eine Förderung zur Beratung von Cyberabwehr (LINK)
Das Mittelstand Digital Zentrum Handel (LINK) informiert in Zukunft regelmäßig über das Thema

Es bleibt also spannend!