



Ansprechpartner: Norman Teichmann
Individualkundenbetreuung

Telefon: 034491 – 680
Telefax: 034491 – 68255
E-Mail: norman.teichmann@vrbank-altenburgerland.de

Datum: 16.02.2024

**VR-Money
Talk**

Cyber ist der Bär, der noch nicht gebrüllt hat

So lautet ein gängiges Mantra an der Wallstreet. Damit ist die Befürchtung einer finanziellen Verwerfung an den Börsen, die durch kriminelle Energie über das Internet ausgelöst wird, gemeint.

Sei es am Arbeitsplatz, im Büro oder zu Hause, wir sind von technologischen Endgeräten und der digitalen Welt abhängig. Die digitale Transformation ist unaufhaltbar und bedeutet für den Großteil der Bevölkerung sich damit auseinander setzen zu müssen. Das macht Cybersecurity zu einem neuen Grundbedürfnis. Auf Grund des zunehmenden Bewusstseins für Datenrisiken und -bedrohungen verzeichnete der weltweite Markt für Cybersicherheit in den letzten Jahren ein robustes Wachstum. Schätzungen zufolge soll der globale Endgeräteschutz-Markt bis 2027 um 8,9 Prozent pro Jahr wachsen.

Immer häufiger nutzen Kriminelle die Schwachstellen der digitalen Welt aus und werden dabei zusehends professioneller.

Cyberkriminalität ist längst ein Teil der weltweit organisierten Kriminalität geworden und hat sich zu einer der größten Bedrohungen für unsere Wirtschaft und Gesellschaft entwickelt.

Die Schäden für die Wirtschaft und Privatleute, die eine Cyberattacke auslöst, sind immens. Der Digitalverband Bitkom beziffert den Schaden für die deutsche Wirtschaft mittlerweile auf über 200 Milliarden Euro jährlich.

Die Angreifer legen Websites von Flughäfen und Behörden lahm, stören das operative Geschäft von Unternehmen und erpressen diese, stehlen Daten,

manipulieren Privatleute und können sogar ganze Kraftwerke stilllegen. Rund jeder fünfte Angreifer schafft es, durch Spam oder Phishing-E-Mails in die Infrastruktur des Unternehmens einzudringen. Oft genügt das bloße anklicken von Links oder das Öffnen von Anhängen durch einen Mitarbeiter, um der Schadsoftware Tür und Tor zu öffnen.

Nicht selten wird der Betrug mittels „Social Engineering“ begangen. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft, Respekt, Angst oder Vertrauen vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Nicht der Computer wird geknackt, sondern der Mensch, der davor sitzt. Der Zweck des Vorgehens ist es, von den Opfern vertrauliche Information zu bekommen, sie zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. In den meisten Fällen ist Geld das Motiv. Die Täter arbeiten auf eigene Rechnung, im Auftrag eines Konkurrenten oder einer Regierung bzw. deren Geheimdienstes.

Die zunehmende Arbeit im Homeoffice und die damit verbundene Verlagerung auf virtualisierte IT-Umgebungen führt bei vielen Unternehmen zu mehr Cyberangriffen. Jedes zweite Unternehmen in Deutschland befürchtet, dass ein erfolgreicher Cyberangriff seine Existenz bedrohen könnte. Das hat dazu geführt, dass Cloudsicherheit, der sich am schnellsten entwickelnde Markt ist. Die Unternehmen, Behörden und die Politik sind gefordert, Antworten auf diese Bedrohungslage zu finden.