Schwachstelle Mensch:

Cyberkriminalität kann JEDEN treffen

Während der Sicherheitsmesse Security in Essen wies NRW-Innenminister Herbert Reul im September darauf hin, dass mittlere und kleinere Unternehmen in Bezug auf Cyberkriminalität nicht gut geschützt seien. Das Schutzniveau sei in den letzten Jahren sogar gesunken, was mit der Corona-Pandemie zusammenhängen könnte, da hier, oftmals ohne sichere Vorbereitungen, Firmenhard- und -software ins Homeoffice verlagert wurde. Das Lagebild Wirtschaftsschutz, erstellt von der Fachhochschule des Mittelstandes in Bielefeld, befragte mehr als 1.000 Unternehmen und stellte fest, dass das Schutzniveau im Vergleich zu 2019 von 4,81 auf 4,41 (Höchstwert der Skala = 10) gefallen ist.
Die Schäden durch Cyberkriminalität haben sich im Vergleich zu 2018/19 fast verdoppelt und betragen jetzt rd. 220 Mrd. Euro.
Gründe hierfür liegen in der gesamtgesellschaftlichen Situation. In einer Studie von Deloitte aus dem Jahr 2020 werden *„Fake News"* als stärkte Bedrohung (74%) angesehen, gefolgt von Datenbereichen (70%), Diebstahl privater Daten / Informationen (67%) oder Viren / Schadsoftware (65%).
Erst kam die Corona-Krise mit der Homeofficepflicht, dann folgte der Ukrainekrieg, der erste Krieg, der auch im Cyberspace geführt wird. Es gibt Angriffe auf die Infrastruktur, nicht nur der kriegführenden Länder, teilweise auch von staatlichen Organisationen. 60% aller Angriffe kommen von organisierten Gruppen und laufen automatisiert ab. Hier werden einerseits Strukturen angegriffen, weniger einzelne Unternehmen oder Personen; andererseits gibt es aber auch sehr gezielte Angriffe, die professionell vorbereitet und nicht leicht zu erkennen sind.
Cyberkriminelle gehen oft sehr professionell vor. Es gab Fälle, in denen erst die Höhe der Versicherung gehackt wurde und dann genau dieser versicherte Betrag gefordert wurde. Auch wird manchmal Hilfestellung geleistet, um nach erfolgter Zahlung das System schnell wieder ans Laufen zu bringen.
Es ist eine Underground Economy (besser bekannt als Darknet) entstanden, die alles im Angebot hat: von Impfnachweisen, über Kreditkartendaten, Kontoinformationen, Passwörtern … Der Zugang zum Darknet ist außerdem deutlich leichter geworden.

Definition Underground Economy = Gesamtheit der Plattformen und Services, welche von Cyber-Kriminellen genutzt werden, um Daten, Tools, Jobs und relevantes Täter-Know-How anzubieten oder in Anspruch zu nehmen. Sie ist Grundlage vieler Straftaten.

Welche verschiedenen Angriffe gibt es?

Oft werden Menschen manipuliert durch Ausnutzen menschlicher Eigenschaften wie Neugier, Angst, Hilfsbereitschaft. Es wird Handlungsdruck erzeugt. Es findet Social Engineering statt.
Social Engineering: Mitarbeiter dazu verleiten, Passwörter und Zugangsdaten preiszugeben, Kontaktaufnahme per E-Mail, Telefon oder soziale Netzwerke.
Häufig wird Ransomware aufgespielt, die den Rechner verschlüsselt. Dann wird Lösegeld für die Datenfreigabe gefordert. Problem ist, dass man nie sicher sein kann, ob die Daten auch wirklich freigegeben werden.
Schäden 2021: 24,3 Mrd Euro (2019: 5,3 Mrd. Euro);
Einnahmen 2021: 602 Mrd. US-Dollar in Krypowährungen. 36% der erpressten Unternehmen haben Lösegeld bezahlt. Der Anteil derer, die danach wieder arbeiten konnten, lag bei rd. 90%.
Die Täter haben erkannt, dass sich die Zahlungsbereitschaft erhöht, wenn die Gegenleistung erbracht wird.
Cyberangriffe sind kein vereinzeltes Phänomen, sie sind flächendeckend.
2020 waren 67% der Unternehmen in Deutschland von Ransomware-Angriffen betroffen.
Phishing durch kontaminierte E-Mails, Fake Internetseiten SMS, Social Media, Telefonie = Abgreifen von sensiblen Zugangsdaten.
DDoS-Angriffe: Server werden mit Anfragen überhäuft und so lahmgelegt – Die Zahl der Angriffe stieg um 41%.
Supply-Chain-Angriffe (Lieferkettenangriffe): Diese sind sehr komplex und verbreiten sich sehr schnell, sie richten sich nicht auf ein bestimmtes Ziel.

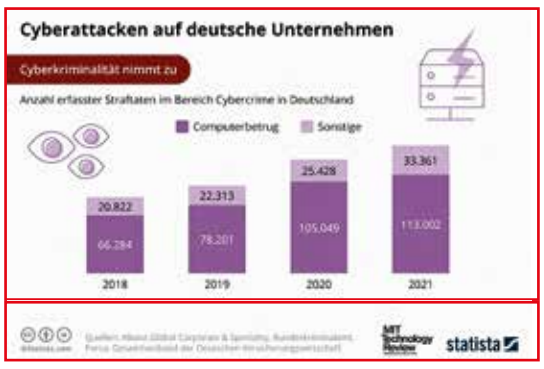
Handlungsempfehlungen

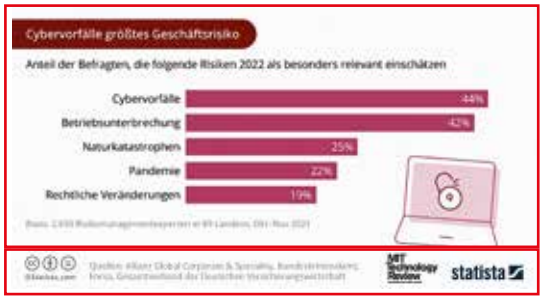
Es ist kein 100%iger Schutz möglich, aber der wichtigste Schutz ist die Sensibilisierung aller Mitarbeiter – vom Praktikanten bis zum Chef.

- Systeme aktuell halten durch regelmäßige Updates,
- Virenschutzprogramm mit regelmäßigen Aktualisierungen,
- Firewall,
- nur mit eingeschränkten Konten ins Internet gehen (keine Administratorrechte),
- komplexe Passwörter (Kleinschreibung, Großschreibung, Ziffern, Sonderzeichen) nutzen,
- ggf. eine 2-Faktor-Authentifizierung einführen,
- Datenträger verschlüsseln,
- digitale Signaturen verwenden (intern und extern),
- auf Auffälligkeiten achten, betroffene Rechner vom Netz trennen,
- regelmäßig Backups machen und auf Funktionsfähigkeit prüfen,
- Mitarbeiter sensibilisieren / schulen.

Verhaltenstipps für Mitarbeiter und Chefs

- Halten Sie sich an die IT-Vorgaben.
- Geben Sie vertrauliche und persönliche Informationen nur sehr zurückhaltend preis.
- Bewahren Sie sich ein gesundes Misstrauen, scheuen Sie sich nicht vor Rückfragen.
- Achten Sie bei eingehenden Mails auf den Absender und die korrekte Schreibung der Adresse.





- Öffnen Sie verdächtige Mails nicht.
- Klicken Sie nicht unbedacht auf Links oder Anhänge.

Schutzmaßnahmen:

1.) E-Mail-Filter einsetzen, 94% der Cyberangriffe kommen über E-Mails,
2.) E-Mail-Attacken erfordern in der Regel eine Reaktion des Mitarbeiters, d.h. Mitarbeiter schulen.
3.) Nötig ist ein intelligenter Endgeräteschutz, der stetig auf verdächtiges Verhalten prüft und ggf. Daten wieder herstellen kann. Alle smarten Geräte müssen geschützt werden, auch Smartphones.
4.) Segmentieren Sie das Netzwerk, damit sensible Bereiche von denen, die viel E-Mail-Kontakt nach außen haben, getrennt sind.
5.) Backup-Management: Ein automatisiertes Hochladen in die Cloud reicht nicht, denn wenn Hacker im System sind und das Admin Passwort haben, können sie auch darauf zugreifen. Es muss ein echtes Offline-Backup installiert werden.

Plan für den Worst case

Viele meinen, dass sie „zu klein" seien, um angegriffen zu werden, aber Hacker gehen oft automatisiert vor und interessieren sich nicht für die Unternehmensgröße, sondern nur für die Schwachstellen. Deshalb muss es einen Notfallplan geben.
Was muss wann getan werden? Wer muss informiert werden? Denken Sie ggf. auch an eine öffentliche Bekanntgabe, um das Vertrauen der Kunden und Geschäftspartner nicht zu verlieren.
Es muss evaluiert werden, welche Systeme den meisten Schutz brauchen, weil sie für den Bestand des Unternehmens essentiell sind. Die Auswirkungen müssen geprüft und in eine Rangfolge gebracht werden. Nicht alles ist gleich wichtig. Gehälter können als Abschlagszahlung gezahlt werden, aber wenn die Produktion stillsteht, keine Waren geordert / geliefert werden können, dann muss es einen Plan B geben. Diese Notfallpläne verursachen in der Regel zwar mehr Arbeit und auch Kosten, dienen aber der zügigen Weiterarbeit nach einem Angriff.
Wichtig sind Versicherungen gegen Cyberkriminalität. Vor Abschluss einer Cyberversicherung sollten Sie unbedingt die Konditionen überprüfen: was genau ist versichert, wie hoch ist die Eigenbeteiligung, ist eine Betriebsunterbrechung versichert, sind Lösegelder auch versichert etc. Nutzen Sie die Angebote unseres Partners deas, Ansprechpartner Dirk Hemmer.

Mehr Informationen unter https://www.zhh.de/intern/service/rahmenabkommen.html.

Weiterführende Informationen

Sie finden u.a. auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder des Bundeskriminalamtes Informationen zum Grundschutz

- Sicherheitscheck des GDV: www.gdv.de/de/Themen/News/Cyber-sicherheitscheck-42702
- Bundesamt für Sicherheit in der Informationstechnik: www.bsi.bund.de
- Verein Deutschland sicher im Netz: www.sicher-im-netz.de.

Sie können auch einige Informationsschriften als pdf in der Geschäftsstelle bekommen: claudia.koch@zhh.de.