Cyberangriffe sind unsichtbar! Das macht sie so gefährlich.

Cyberkriminalität in Zeiten von KI

Wie kommt die Schadsoftware ins Unternehmen?

Cyberkriminalität beschäftigt uns, seitdem es das Internet gibt. Anfangs waren die Bedrohungen selten, viele verzichteten auf Schutzmaßnahmen. Inzwischen dürften die Quoten an Firewalls, Virenscannern und anderen Schutzmechanismen die 100%-Marke erreicht haben. Diese Systeme filtern viele Angriffe heraus, manche schaffen es allerdings bis auf einzelne Rechner zu kommen. Meistens versteckt in einer E-Mail.

Jetzt ist die menschliche Intuition und das Wissen über Auffälligkeiten gefordert, solche Mails zu erkennen. In der Vergangenheit fielen diese E-Mails durch fehlerhaftes Deutsch, falsche URL sowie ein laienhaftes Layout etc auf. Heute werden sie oft von KI gestaltet und sind auf den ersten Blick nicht als Fake zu erkennen – höchstens vielleicht an der korrekten Rechtschreibung. Nach wie vor gilt: Das größte Risiko sitzt vor dem Rechner.

Durch KI werden die Attacken auch schneller und häufiger. Die Reaktionen sollten auch schneller erfolgen. Dies bedeutet, dass Schutzprogramme immer aktuell gehalten werden müssen und dass – auch mittels KI – Schwachstellen identifiziert und eliminiert werden müssen.

Weitere Gefahren drohen durch die ungeprüften Nachrichten auf den Social Media, die dann in allen Medien weiterverbreitet werden. Bevor solche Informationen weiterverbreitet werden, muss im Grunde erst der Wahrheitsgehalt geprüft werden. Die KI-VO schreibt zwar die Kennzeichnung von KI-generierten Inhalten vor, aber welcher Kriminelle hält sich schon an Gesetze und Verordnungen?

Das Leben ist deutlich komplizierter geworden, und viele sind verunsichert, was sie überhaupt noch glauben können. Bevor irgendwelche Informationen geteilt werden, sollten sie durch verschiedene Quellen verifiziert werden, damit Sie nicht zum Multiplikator der Fake News werden.

Bis 2022 hat Künstliche Intelligenz in der deutschen Wirtschaft kaum eine Rolle gespielt. Aber mittlerweile hat das Thema Fahrt aufgenommen, wie aktuelle Zahlen des Digitalverbands Bitkom zeigen.

Schutzmaßnahmen

Wie in der realen Welt können Sie auch im Cyberspace das Risiko nicht auf Null setzen, aber Sie können es minimieren und die Sicherheit erhöhen. Wichtig ist zuallererst die Information. Die Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die Seiten der Polizei und des Bundeskriminalamtes (BKA) zeigen eine Reihe von Maßnahmen auf. Prüfen Sie, was für Ihr Unternehmen passt, und setzen Sie die Maßnahmen um.

- Aktualisieren Sie Ihr Betriebssystem und die genutzten Programme regelmäßig.
- Nutzen Sie unbedingt die Sicherheitsupdates.
- Ein immer aktueller Virenschutz sowie eine Firewall sind unverzichtbar.
- Verwenden Sie komplexe Passwörter (Ein regelmäßiger Wechsel wird inzwischen als unnötig erachtet, da viele nur marginale Änderungen an ihren Passwörtern vornehmen.), die im Falle eines Hacks umgehend geändert werden müssen.
- Verschlüsseln Sie Ihre E-Mails und verwenden Sie digitale Signaturen in der internen und externen Kommunikation.
- Achten Sie auf Auffälligkeiten, trennen Sie infizierte Systeme vom Rest.
- Erstellen Sie regelmäßig Backups, bewahren Sie sie längere Zeit auf, bevor sie überschrieben werden.
- Testen Sie im Normalbetrieb, ob sich die Backups problemlos installieren lassen.

Ein wesentlicher Faktor sind – genauso wie im realen Leben – die (ehemaligen) Mitarbeiter. In den weitaus meisten Fällen ist es keine kriminelle Energie, sondern Fahrlässigkeit und Unwissenheit. Es gibt spezielle IT-Schulungen, die die Kompetenzen erhöhen. Grundsätzlich sollten Sie ihren Mitarbeitern folgende Tipps geben – und auch selbst beachten:

- Seien Sie vorsichtig, mit der Weitergabe von vertraulichen und persönlichen Informationen.
- Nutzen Sie Ihren gesunden Menschenverstand und fragen Sie nach, wenn Ihnen etwas komisch vorkommt. Besser einmal zuviel, als einmal zuwenig fragen.
- Prüfen Sie E-Mailadressen im Hinblick auf den Absender und die Domain.
- Öffnen Sie verdächtige Mails nicht, ebenso keine Anlagen von Unbekannten.
- Auch beim Anklicken von Links sollten Sie vorsichtig sein. Manche gefälschten Mails sehen den originalen sehr ähnlich, so dass ein genaues Hinsehen erforderlich ist. Oftmals verrät die Absenderadresse die Fälschung.

Kriminelle reagieren häufig auf allgemeine Situationen; z.B. werden derzeit Mails zu angeblichen Kontoaktualisierungen versendet, um an Zugangsdaten zu kommen. Noch immer werden mit Ransomware, also Makroviren, die Computer oder auch ganze Systeme verschlüsselt und nur nach Zahlung einer Geldsumme (häufig in Bitcoins) wieder entschlüsselt – oder auch nicht. Diese Erpressungssoftware ist im Vorfeld schwierig zu identifizieren, da sie von normalen Virenscannern oft nicht erkannt wird. Es gibt Programme, die PC-Systeme in Echtzeit überwachen und auf untypisches Verhalten reagieren.

Besser ist es, in Firmensmartphones zu investieren, als das Nutzen privater Geräte zu erlauben. Die Firmensmartphones können mit Sicherheitssoftware und Verschlüsselungen versehen werden und so auch privat genutzt werden.

Auch Telefonanlagen können gehackt werden und dann wird auf Ihre Kosten telefoniert.

Welche Angriffe drohen?

Im vergangenen Jahr lagen auf den ersten beiden Plätzen KI-gestützte bösartige Angriffe und KI-gestützte Desinformation. Schurken-KI (Rogue AI) ist KI, die gegen die Ziele des Anwenders agiert. Dies kann einerseits quasi aus Versehen passieren, wenn falsche Eingaben gemacht werden oder Angreifer haben die Programme infiziert, um Schäden auszulösen.

Betrugsautomatisierung. Schon in der Vergangenheit gab es Phishing-Mails, die versucht haben, Daten abzugreifen oder Rechner zu sperren, um Lösegeld zu erpressen. Oft waren sie schnell zu identifizieren: durch ein falsches Layout, durch falsche Ansprache, durch falsche Logos etc. Durch KI werden diese Angriffe deutlich ausgeweitet, sowohl in der Anzahl, der Genauigkeit, der Personalisierung als auch in der Reichweite.

Das BSI unterscheidet drei Kategorien von Angriffen mit KI-Unterstützung:

- KI wird eingesetzt, um Informationen zu sammeln, dann ausgewertet und Schwachstellen werden ausgenutzt oder Fake News verbreitet.
- Es werden unternehmenseigene KI-Systeme angegriffen, um sensible Daten zu erlangen.
- Mitarbeiter nutzen KI unreflektiert und unautorisiert, dies kann dann mit infizierten KI-Tools geschehen.

Enormer finanzieller Schaden

Der Schaden durch Cyberattacken ist zudem immens: Laut einer Erhebung des

Verbands Bitcom verursachten sie 2024 Schäden in Höhe von 178,6 Milliarden Euro. Das sind 30 Milliarden mehr als im Vorjahr.

Auswirkungen auf Schadsoftware durch KI

- Die Entwicklung von Schadsoftware jeder Art wird leichter und schneller.
  (Im vergangenen Jahr war es laut BSI noch fraglich, ob KI selbständig neue Schadsoftware schaffen kann.)
- Durch KI wird die Schadsoftware modifiziert und verschleiert, so dass sie schwerer zu entdecken ist.
- KI löst Captchas und gaukelt vor, ein Mensch zu sein.
- KI findet Passwörter schneller heraus.

Durch KI wird die Bedrohungslage verändert. Es finden technische Veränderungen statt und ebenso Social-Engeneering-Angriffe (Persönliche Angriffe). Der Umfang und die Geschwindigkeit der Angriffe nimmt zu, auch steigt die Qualität der Angriffe. Mit KI generierte E-Mails sind viel schwerer zu erkennen, als die bekannten Phishing-Mails, da sie täuschend echt gemacht werden können. Wer der KI die richtigen Prompts liefert, der wird erschreckende und gleichzeitig faszinierende Ergebnisse erhalten. KI hat kein Gewissen, keine Ethik oder Moral, sie erstellt Schadprogramme genauso wie nützliche Programme. Ihre Arbeit hängt von dem ab, der sie mit Informationen füttert.

Selbst auf den ersten Blick harmlose KI wie zum Beispiel das Übersetzungsprogramm deepl kann einerseits im internationalen Geschäftsbetrieb oder auch mit Mitarbeitern, die der deutschen Sprache noch nicht ausreichend mächtig sind, außerordentlich nützlich sein. Aber andererseits werden Phishing-Mails, deren Urheber häufig nicht aus Deutschland kommen, sondern global agieren, nahezu perfekt übersetzt, so dass es immer schwerer wird, anhand der Sprache eine bösartige Mail zu identifizieren. Böse Zungen behaupten, dass eine korrekte Rechtschreibung heutzutage ein Indiz für eine Fake-Nachricht ist.

Nachrichten werden immer besser personalisiert, ein angemessener Sprachstil verwendet, die Rechtschreibung geprüft, plausible Domainnamen oder URL generiert. Deep Fakes gibt es in allen Bereichen, in Text, Bild und Ton. Schon ein Sprachschnipsel von 15 Sekunden Länge reiche professionellen Hackern, um ganze Reden zu generieren, so Florian Arndt auf dem 8. PVH-Kongress in Köln. Diese klingen dann wie das Original, nur die Inhalte sind es nicht.

Weiterbildung

Es ist überaus wichtig, dass die Mitarbeiter geschult werden, nicht nur im Umgang mit KI, sondern auch darin, möglicherweise von KI geschaffene Werke zu erkennen.

Das Gesetz schreibt eine Kennzeichnungspflicht vor, aber welcher Kriminelle hält sich schon an Gesetze?

KI ist letztendlich ein Werkzeug, das die Arbeit erleichtert oder erschwert. Der Umgang muss erlernt, Risiken müssen erkannt werden. Wer unternehmensinterne Daten, seien es technische Daten, seien es personenbezogene Daten, nutzt, um mit der KI schneller zu arbeiten, der muss damit rechnen, dass diese Daten in öffentliche Datenbanken eingelesen werden. Hier dürfen nur explizit gesicherte Programme genutzt werden, bzw. es darf für solche Anwendungen, die oftmals Automatisierungen sind, keine Anbindung an das Internet existieren.

Schutzmaßnahmen

- Informierte Mitarbeiter
- Skeptische und wachsame Mitarbeiter
- Hoher Datenschutz und Kontrolle, ob er auch eingehalten wird
  Da generative KI, wie z.B. ChatGPT, durch jeden Prompt dazu lernt und sein Wissen erweitert, können Kriminelle sich durch Eingabe entsprechender Prompts unrechtmäßig Daten verschaffen und diese dann für Angriffe nutzen.

Initiative IT-Sicherheit

Mit der Initiative IT-Sicherheit in der Wirtschaft unterstützt das Bundesministeriums für Wirtschaft und Energie Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere kleine und mittelständische Unternehmen (KMU) werden für das Thema sensibilisiert und durch konkrete Hilfsangebote bei der Erhöhung ihres IT-Sicherheitsniveaus unterstützt.

Im Zentrum steht hierbei die Transferstelle Cybersicherheit im Mittelstand. Hier werden passgenaue Informationen aus einer Hand geliefert. Sie bündelt, bereitet praxisnah auf und vermittelt Angebote zum Thema IT- Sicherheit und unterstützt kleine und mittlere Unternehmen, Handwerksbetriebe und Selbstständige bei deren Umsetzung.

Der neue BSI-E-Mail-Check

E-Mails sind mit 90% das Hauptziel von Cyberangriffen, egal ob es um Identitätsdiebstahl, Spionage oder um das Einschleusen von Schadcode geht – deshalb hat das Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein Online-Tool entwickelt, das zeigt, ob moderne Sicherheitsstandards erfüllt werden.

Das BSI hat zwei Richtlinien erarbeitet, in denen Kriterien festgeschrieben wurden, die für einen sicheren Transport von E-Mails und für eine sichere Authentifizierung sorgen sollen. E-Mail-Programme sollen künftig erkennen können, von wem eine Nachricht geschickt wurde und ob dessen Adresse womöglich gefälscht ist. Hierdurch können sich Kriminelle nicht mehr hinter dem Empfänger bekannten E-Mail-Adressen verstecken.

Susanne Dehmel, Mitglied der Geschäftsleitung des Digitalbranchenverbandes Bitkom: *„Nur wenn E-Mails wirksam abgesichert sind, sind Geschäftsprozesse sowie Kundendaten geschützt und wird das Vertrauen in digitale Dienste gestärkt."* 26 Prozent der Unternehmen in Deutschland hätten in den vergangenen zwölf Monaten Schäden durch Phishing erlitten. Besonders von kleinen Betrieben wird das Risiko von Cyberangriffen häufig unterschätzt.

Wie die Initiatoren der Kampagne für sichere E-Mails mitteilten, erreichen jedes berufliche Postfach täglich im Schnitt 42 E-Mails. 90% aller Cyberangriffe kommen über den E-Mail-Verkehr.

Auch durch Fake-Internetseiten, die die Eingabe von persönlichen Daten fordern oder das Öffnen von Links auf unseriösen Seiten, kann Schadsoftware auf den Rechner bzw. in das Firmennetzwerk gelangen.

Reaktionen

Sollte ein Angriff erfolgreich gewesen sein, dann sollten Sie einen Reaktionsplan vorliegen haben, der schnell umgesetzt werden muss. Dieser Notfallplan muss zusammen mit den Compliance- bzw. Datenschutzbeauftragten und ggf. dem Betriebsrat sowie der Rechtsabteilung erarbeitet werden. Lassen Sie sich ggf. von externen Fachleuten beraten. Jeder Mitarbeiter sollte den Plan kennen und ggf. anwenden können.

Cybercrime kann jeden jederzeit treffen, deshalb müssen Sie für den Ernstfall konkrete analoge Handlungsregelungen parat haben.

Cyberversicherungen

In Anbetracht der hohen Bedrohung durch Cyberkriminalität machen inzwischen viele Versicherungen Angebote, die die Risiken minimieren sollen. Diese sind – wie alle Policen – genau zu prüfen, ob sie die benötigten Risiken abdecken.

Häufig sind sie nach dem Baukastenprinzip angelegt. Auch unser Rahmenabkommenspartner **deas** bietet eine Cyberversicherung zu vergünstigten Konditionen für ZHH-Mitglieder an.

Kontakt:
Martin Müdder, Kundenbetreuer,
deas Deutsche Assekuranzmakler GmbH
Josef-Lammerting-Allee 12, 50933 Köln
Telefon: 0221.67082169
E-Mail: martin.muedder@deas.de

Begünstigende Faktoren

Da sowohl technische als auch menschliche Faktoren eine Rolle spielen, muss auf beiden Ebenen präventiv gearbeitet werden. Zunehmende Komplexität der Technik und Unachtsamkeit der Mitarbeiter sind Hauptgründe für erfolgreiche Cyberangriffe.

Weitere Informationen können Sie in der Geschäftsstelle bei Natasa Röhle bekommen: natasa.roehle@zhh.de.