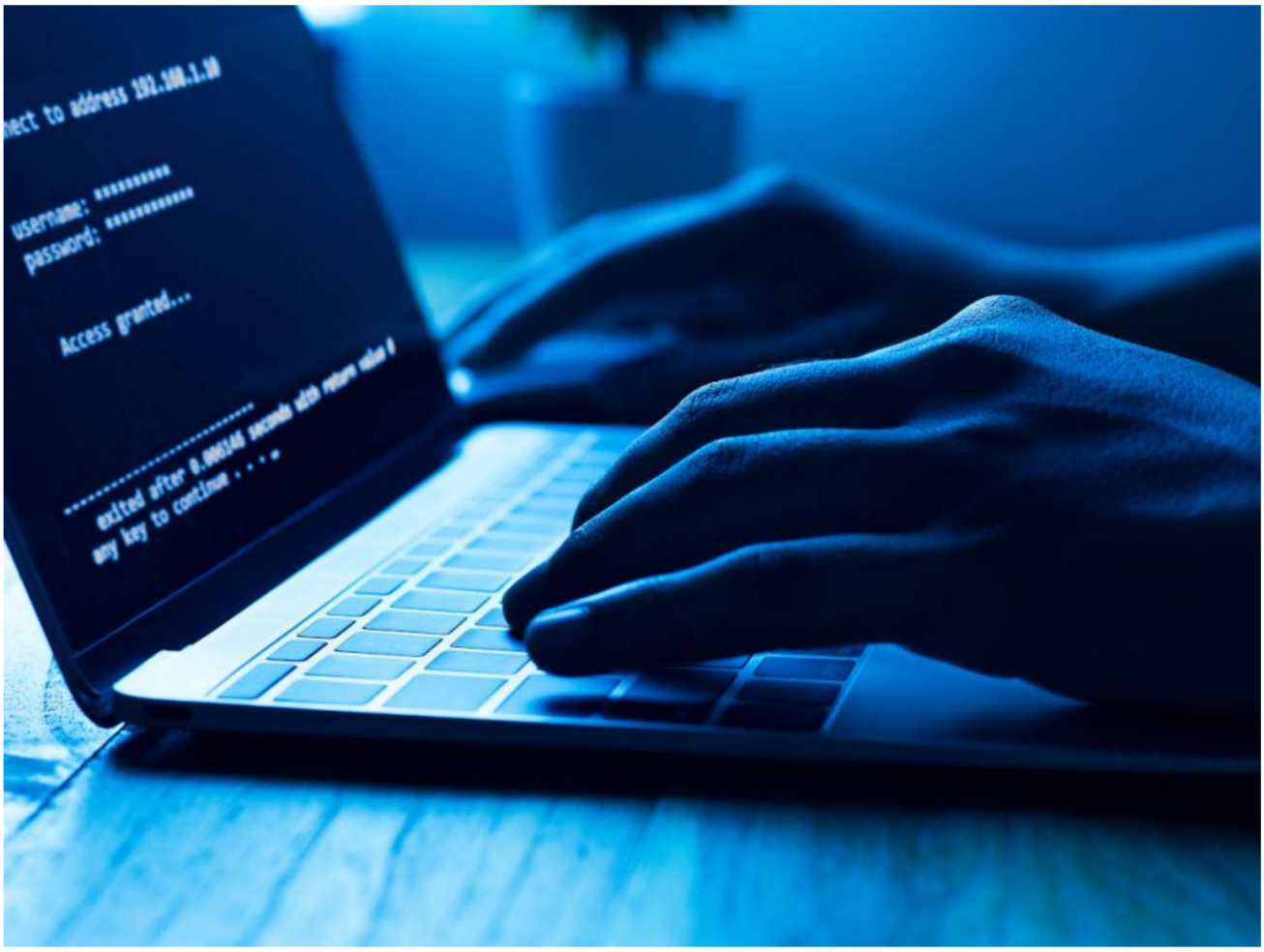
Wirtschaft

12. Apr. 2022 | 08:49 Uhr | von Siegfried Müller

Verschärfte Lage wegen Ukraine-Krieg

Hackerattacken: Was Firmen jetzt tun müssen

Infolge des Ukraine-Krieges ist die Bedrohung durch Hacker gestiegen. Wie sich Firmen kurz- und langfristig wappnen, erklärt unser Kolumnist Siegfried Müller.



Was hilft wirklich gegen Hackerangriffe? Das erklärt Cybersicherheits-Experte Siegfried Müller in seiner Kolumne. (Bild: stock.adobe.com - JaRiRiyawat)

Wahrscheinlich erzähle ich Ihnen jetzt tatsächlich erst einmal nichts neues. Das Thema Cyber-Risiken im Zusammenhang mit der aktuellen Situation ist so allgegenwärtig – dem lässt sich kaum ausweichen. Dabei haben die Beiträge der letzten drei, vier Wochen ungefähr alle den gleichen Tenor: Unternehmen müssen auf eine abstrakt höhere Gefahrenlage vorbereitet sein oder – mit anderen Worten – darauf, dass sich die „Bedrohungslage im Cyberraum verschärfen wird".

Ebenso häufig wird darauf hingewiesen, dass in der Regel jedes dritte Unternehmen, also 34 Prozent – manchmal wird hierzu auch mal eine niedrigere oder höhere Zahl zitiert – seine IT-Schutzmaßnahmen kurzfristig hochgefahren hat. Natürlich ist es momentan mehr als angebracht zu sichten, inwieweit das eigene Unternehmen gegen die Cyberangriffe gewappnet ist und einige Schutzmaßnahmen, die sich schnell umsetzen lassen, tatsächlich schleunigst zu realisieren. Denn schließlich gaben – laut einer Umfrage vom Bitkom – 17 Prozent der Unternehmen an bereits konkrete Anzeichen für einen Angriff erkannt zu haben.

Es ist also auf jeden Fall vernünftig kurzfristig zu reagieren, denn alles was in der augenblicklichen Lage umgehend zur Stärkung des Schutzniveaus beiträgt, kann nur positiv bewertet werden. Andererseits perspektivisch gesehen hat dies keinen Bestand, denn grundlegende Entscheidungen über Maßnahmen zur Erhöhung der IT-/Cyber-Sicherheit lassen sich nicht ad hoc treffen – Sie müssen agieren, denn hier bedarf es einer strukturierten Analyse, um den tatsächlichen Schutzbedarf zu ermitteln und diese Erkenntnisse in die Sicherheitsstrategie entsprechend zu adaptieren. Oder wie es im Fact Sheet herausgegeben von "The White House" formuliert wird: "bake it in, don't bolt it on". Was wörtlich übersetzt „einbacken, nicht anschrauben" bedeutet und die Sache damit auf den Punkt bringt.

Kann man sich noch gegen Cyberattacken versichern?

Adaptieren ist übrigens ein gutes Stichwort, denn wie sich aktuell zeigt, ändern sich Gegebenheiten manchmal schnell. Vor einigen Wochen habe ich noch sagen können, dass eine Cyberversicherung unter verschiedenen Aspekten empfehlenswert sei, auch weil die darüber abgesicherte Schadensabdeckung als Wettbewerbsvorteil verargumentiert werden könne. Doch hier ist – Stand jetzt – als neue Dimension nun zu beachten, dass, proportional zu der wachsenden Gefahr von Hackerangriffen im Cyberraum, die Versicherbarkeit der Cyberrisiken abnimmt. Allein aus dem Grund, dass anlässlich der geänderten Umstände viele Versicherer hohe Verluste befürchten.

Was sich hingegen immer noch als hilfreich erweisen könnte ist, die erworbene Expertise von Cyberversicherern bezüglich geeigneter Schutzmaßnahmen gegen potenzielle Bedrohungen zu nutzen.

Aktuelle Bedrohungen und was Unternehmen ad hoc dagegen tun können

Dies sind – nach wie vor – in der Hauptsache zwei Angriffsvektoren: Phishing und Ransomware. Um hier die Effektivität zu erhöhen, wird über Social Engineering die anvisierte Zielperson geschickt mithilfe von Phishing-Mails manipuliert, etwa um Informationen preiszugeben oder bestimmte Handlungen auszuführen, die im Weiteren einen Angriff ermöglichen – beispielsweise das Platzieren von Malware.

Auch wenn Ihnen diese Angriffsmethoden und -mechanismen allgemein geläufig sein mögen, so müssen Sie bedenken, dass die Cyberkriminellen diese natürlich kontinuierlich verändern. Zum Beispiel beim Phishing werden nicht nur die Inhalte jeweils stark (emotionalisiert) an die aktuelle Interessenlage angepasst, sondern es gibt hier auch eine rege Diversifikation – vom Spear-Phishing*, über Whaling* und Chamäleon-Phishing* bis hin zu Vishing*. Da ist es nicht immer leicht den Überblick zu behalten und Mitarbeiter davor zu bewahren, nicht darauf reinzufallen.

3 Tipps gegen Hacker: Wie sich Angriffsflächen verringern lassen

Von daher ist es notwendig – gerade jetzt, in diesen eindeutig außergewöhnlichen Zeiten – Investitionen in Cyber-Sicherheitsmaßnahmen nicht auf die lange Bank zu schieben und parallel dazu umgehend damit zu beginnen, sowohl das Risiko von Cyberangriffen zu reduzieren als auch mit den verbleibenden umzugehen.

Sie können sofort damit anfangen Ihre Angriffsflächen zu verringern, denn einige Maßnahmen lassen sich ad hoc durchführen:

1. Teilweise wird Software, beziehungsweise werden Programme und Apps, nur zur einmaligen Verwendung heruntergeladen => überprüfen Sie Ihre IT-Systeme dahingehend und entfernen Sie unnötige Software, beziehungsweise Programme und Apps.
2. Oftmals sind Berechtigungen erteilt worden, die zu einem späteren Zeitpunkt weder eine Gültigkeit noch eine Notwendigkeit haben, so kommt es beispielsweise nicht selten vor, dass ausgeschiedene Mitarbeitende stellenweise noch über Zugriffsrechte verfügen => überprüfen Sie die Rechtevergabe sorgfältig sowie kritisch und schränken Sie Zugriffsrechte gemäß der angemessenen Erforderlichkeit ein.
3. In Routern oder Firewall-Systemen werden zum Beispiel für Testzugänge Ports geöffnet, um die notwendige Kommunikationsmöglichkeit zu schaffen, ohne diese im Anschluss wieder zu schließen => reduzieren Sie die Kommunikationsmöglichkeiten durch Einstellungen in Ihren Routern und Firewall-Systemen.

Was zu tun ist, wenn das Unternehmen von einem Hacker attackiert wird

Für den Fall, dass Ihr Unternehmen angegriffen wird, gilt es, so schnell als möglich Maßnahmen zu ergreifen, um die Auswirkungen des Angriffs einzudämmen. Die nachfolgend genannten können Sie sofort vorbereiten:

1. (Halb-)automatisierte Reaktion auf Angriffe

Wenn ein Angriff erkannt wird, ist es sinnvoll, umgehend – und möglichst (halb-) automatisiert – Firewall- und/oder E-Mail-Server-Regeln so einzuschränken, dass nur noch die tatsächlich relevanten Prozesse des Unternehmens aufrechterhalten werden können. Verfassen Sie ein Konzept, in dem die relevanten Prozesse ihres Unternehmens beschrieben sowie die notwendigen Regeln definiert sind.

2. Einsatzplanung der Mitarbeitenden

Wenn ein Vorfall eingetreten ist, wird es auf jeden Fall notwendig sein, dass genügend qualifizierte Mitarbeitende vor Ort sind um die notwendigen Schritte einleiten und Maßnahmen durchführen zu können. Erstellen Sie einen entsprechenden Notfall-/Einsatzplan, um zu gewährleisten, dass alle Zuständigkeiten genau definiert sind und so eine zeitnahe Reaktion möglich ist.

Was noch aus der Situation resultiert

Die aktuelle Situation hat einen weiteren Nebeneffekt, womit anfangs keiner gerechnet hat – im wahrsten Sinne des Wortes: Die enorme Steigerung der Energiekosten. Weitergedacht bedeutet das, Dienstreisen werden erheblich teurer und dies wird vermutlich bei den Auftraggebern zu Buche schlagen.

Das zeigt deutlich, dass Fernwartung nicht nur während der Corona-Zeit bestmöglich geeignet war einen *modus vivendi* für die damaligen Gegebenheiten zu bieten, sondern auch weiterhin im Sinne einer langfristig auf Effizienz ausgelegten Unternehmensstrategie nicht mehr wegzudenken sein wird. Natürlich gilt auch hier, der Sicherheit oberste Priorität einzuräumen. Informationen zum Basis-Schutz bezüglich der Fernwartung erhalten Sie hier.

Mein Fazit

Die beste Zeit sich vorzubereiten ist jetzt – sowohl indem Sie kurzfristig handeln, als auch schnellstmöglich die Planung der notwendigen Maßnahmen und Cyber-Sicherheitsmaßnahmen angehen.

Über den Autor

Kolumnist Siegfried Müller, CEO und Gründer der MB connect line GmbH. (Bild: Siegfried Müller)

Siegfried Müller ist geschäftsführender Gesellschafter der MB connect line GmbH. In seinen ersten Berufsjahren als Steuerungstechniker für den Maschinenbau hat er den Nutzen von Fernwartung erkannt. Im Alter von 25 Jahren gründete er MB connect line. Unter seiner Leitung entwickelte sich das Unternehmen zum Technologieführer in den Bereichen Fernwartung, Datenerfassung und Industrial Security. Seit über 20 Jahren treibt Siegfried Müller mit viel Engagement und Leidenschaft die Entwicklung neuer Produkte und Lösungen für die sichere industrielle Kommunikation über Internet voran. Als Stratege und Experte zur Cybersicherheit im industriellen Umfeld bringt er sein Wissen auch in nationalen und internationalen Arbeitskreisen ein – beispielsweise beim Cluster Mechatronik & Automation Bayern e.V., beim TeleTrusT – Bundesverband IT-Sicherheit e.V. und in der European Cyber Security Organisation (ECSO). Die wichtigen wirtschaftlichen Themen adressiert er als Senator im internationalen Wirtschaftssenat (IWS).