THE UNIFIED
tkuc Group

Ist Ihr Unternehmen wirklich sicher?

Diese Gefahrenquellen werden von den meisten Unternehmen übersehen

Ist Ihr Unternehmen wirklich sicher?

Was sind die häufigsten “Einbruchstore”?

SICHERHEIT

Einleitung

Unternehmen stecken oft sehr viel Geld in die Sicherheit ihrer IT-Systeme, doch ist das Geld gut angelegt? Das meiste Geld wird in Netzwerk-Sicherheit investiert, das größte Sicherheitsrisiko sind jedoch die Mitarbeiter durch Unwissenheit, Neugier und Social Engineering.

Die besten Sicherheitslösungen helfen den Unternehmen beim Schutz gegen Angreifer nicht, wenn diese nicht gut aufgesetzt sind oder diese aufgrund fehlender/knapper Mitarbeiter-Ressourcen nicht so zum Einsatz kommen, wie dies vorgesehen ist.

Diese Eckpunkte sollten Unternehmen auf dem Radar haben:

• Regelmäßige Schulung der Mitarbeiter zu Themen der IT-Sicherheit, idealerweise begleitet durch Phishing-Simulationen

• Gute Backup-Lösungen , die getrennt von den IT-Systemenund offline speichern. Das Backup muss auf einem Medium liegen, dass nicht verschlüsselt werden kann. Das Restore der Daten sollte alle 6 Monate getestet werden

• Systeme müssen auf dem aktuellen Software-Stand sein. Angreifer kennen die Schwachstellen der Betriebssysteme und Anwendungssoftware und nutzen diese gerne rus.

• Systeme müssen bekannt sein – Schatten -IT ist nie auf dem aktuellen Stand und ein Einfallstor für Angreifer

• Least Privilege – Jeder Mitarbeiter sollte nur auf die Applikationen und Daten Zugriff haben, die er für seine tägliche Arbeit benötigt. Der Zugriff auf IT-Systeme sollte nur mit gesonderten administrativen Accounts möglich sein.

• Datenklassifizierung – Es gibt keinen Grund, dass ein neuer Mitarbeiter im Durchschnitt Zugriff auf hunderttausende Dateien hat. Daten sollten klassifiziert sein, damit sensitive Daten besonders geschützt werden können. Der Zugriff auf Daten sollte auf die Rolle limitiert sein.

Eine moderne Firewall Lösung ist natürlich ein Muss für jedes Unternehmen. Neben einem klassischen Regelwerk muss eine moderen Firewall mittels KI Anomalien und verdächtiges Verhalten erkennen und blockieren können. Auch ein Filtering des Internet-Verkehrs sollte die Firewall beherrschen.

Bei 2-Faktor Authentisierung sollten Unternehmen darauf achten, dass Sie es den Angreifern nicht zu einfach machen. Mobil-Telefone sind nicht besonders gut geschützt und damit ein einfaches Ziel für einen Angreifer. Lösungen wie Invisble MFA machen es dem Angreifer deutlich schwerer, dafür dem Mitarbeiter einfacher.

Agentenlose Erkennungs-Systeme (Netzwerk Detection Response) sind notwendig, um Angreifer im Netz detektieren zu können. Da es nie 100% Sicherheit gibt, werden Angreifer Wege finden, um in Ihr Netzwerk zu gelangen. Da es für nahezu alle XDR-Lösungen Möglichkeiten und Tools zum Abschalten oder Bypassen gibt, wird der Angreifer dort nicht erkannt. Agentenlose Erkennungs-Systeme sind unsichtbar für den Angreifer und damit auch nicht abschaltbar.

Was kann man noch besser machen.

Den Fokus sollten Unternehmen auf die Verwaltbarkeit der Systeme legen. Es hilft nichts, wenn Unternehmen teure EDR- (Endpoint-Detection Response) oder XDR- (Extended Detection Response) Lösungen einführen, aber keine Ressourcen für das Management haben. Dann wird aus diesen Systemen eine reine Endpunktschutzerlösung, die nicht einmal besonders sicher ist. Hier kann weniger mehr sein.

Zusätzlich zu den o.g. Sicherheitslösungen empfehlen wir neben einem jährlichen Penetrationstest (Pen-Test) ein Tool, dass die externe Sicherheit permanent überwacht und bei einem Abfall des Sicherheitsniveaus alarmiert.

Ergänzen lässt sich das durch die Darknet-Monitoring, damit eine Alarmierung erfolgt, wenn Unternehmensdaten oder z.B. Logins im Darknet zum Kauf angeboten werden. erkennen. Idealweise kann die Lösung unsicherer Lösungen direkt patchen

Angreifer, die einmal im Netz sind, bewegen sich gerne von Maschine zu Maschine und verwenden dabei die Userdaten von Mitarbeitern. Netzwerk Detetection Lösungen erkennen diese Angreifer, sodass diese ausgesperrt werden können, bevor Schaden entsteht.
Mindestens die Kronjuwelen des Unternehmen sollte durch Mikrosegmentation im Rahmen einer ZeroTrust Strategie geschützt werden.. Moderne Lösungen lernen den Verkehr und erlauben eine risikoarme Einführung. Dies funktioniert in IT-Umgebungen ohne zusätzliche Hardware, lediglich zum Schutz von OT-Systemen werden Hardware-Firewalls benötigt.

Unsere Referenzen

TCS TATA CONSULTANCY SERVICES · Autohaus HERTEN GRUPPE · A. HAAS · Thies · Osterholzer Stadtwerke · LEMKEN · Schmidbauer · Gothaer

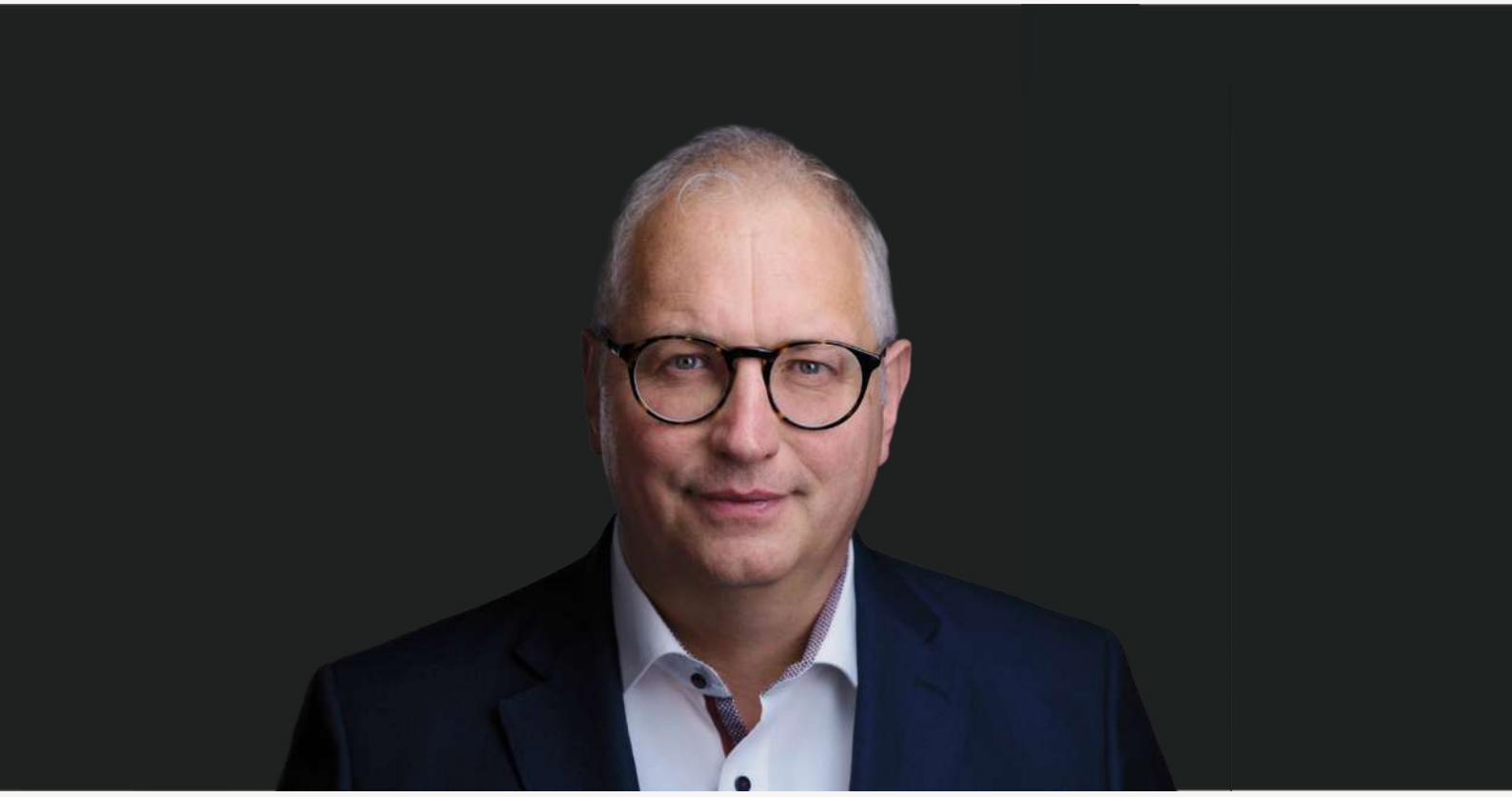
Das Directory des Unternehmens sollte regelmäßig überprüft werden. Zum einem muss überprüft werden, dass Accounts von ausgeschiedenen Mitarbeitern mindestens deaktiviert, besser noch gelöscht sind. Darüber hinaus ist zu validieren, ob ein Least Privilege angewendet wird, oft haben interne und sogar externe Mitarbeiter, viel mehr Rechte und Zugriffe als notwendig. Hier gibt es gute Lösungen, die bei der Ermittlung des benötigten Zugriffs helfen können. Beim On- und Offboarding von Mitarbeiten können entsprechende Prozesslösungen helfen, die dies dann vollkommen automatisch übernehmen.

Da Angreifer in der Regel mindestens 50 Tage, manchmal aber auch weit über 250 Tage im Netz sind, sollte man dies beim Backup berücksichtigen und entsprechende Langzeit-Backups speichern.

Beim Backup ist auch zu berücksichtigen, dass SaaS-Lösungen von Microsoft, Google und anderen kein Backup mitbringen. Auch hier ist es Aufgabe des Kunden die Daten von Azure, Exchange, Dynamics, Power BI oder Google Workspace zu sichern.
SAP ist bei den Unternehmen, die es einsetzen, ein hochkritisches System. Trotzdem wird es bei der IT-Security-Betrachtung häufig ignoriert. Natürlich lassen sich bei SAP viele Daten aus Logs lesen, aber haben Sie die Mitarbeiter die dies so korrelieren können, dass Sie Schwachstellen und Anomalien erkennen?

Ein oft unterschätztes Risiko bringt die Supply-Chain mit sich. Neue und unternehmenskritische Lieferanten werden bei den meisten Unternehmen hinsichtlich ihrer wirtschaftlichen Kennzahlen geprüft. Teilweise werden auch ein paar Cyberrisiken abgefragt, wobei sich dies häufig auf Zertifizierungen beschränkt. Wir empfehlen den Einsatz entsprechender Lösungen, mit denen validiert werden kann, ob die Unternehmen sich auch tatsächlich um ihre Risiken kümmern.

Neben den internen IT-Sicherheitsrisiken, die zwischen der Firewall, Cloud und dem User liegen, gibt es auch die, viel zu selten betrachtete, externe Sicherheit. Hierbei geht es nicht um den Wachdienst, sondern um den Schutz der Marke, der handelten Personen, ihre Domänen, Social Media Auftritte, nicht erkannte Daten-Leaks, Daten von Unternehmens-Kreditkarten oder auch die Internet Infrastruktur. Wenn ihre Daten im Darknet verkauft werden oder Aktionen gegen Mitarbeiter, die Marke oder ihr Unternehmen im Ganzen vorbereitet werden, dann sollten Sie dies kennen, solange Sie noch reagieren können. Auch wenn jemand ähnliche Domänen registriert oder sogar versucht ihre zu übernehmen, zählt jede Sekunde.



Thomas Kress
Geschäftsführer
+49 (0) 6021 441 215
thomas.kress@theunified.de
www.theunified.de

Jetzt Termin vereinbaren