Cyberangriff auf das EDV Netzwerk der Firma EAM in der WOLF Gruppe:

Montag, 1.4.2024

Bei der Überprüfung der Sicherheits-Logs wurde festgestellt, dass Verschlüsselungstechnologie einige Dateien auf Servern verschlüsselt hatte. Der Angriffsvorgang war zu diesem Zeitpunkt bereits von einem internen, automatisierten Mechanismus beendet worden.

Im Zuge des Angriffs wurden alte, interne Kontaktadressen entwendet, und damit ein Bekennerschreiben an einige Mitarbeiter*innen versandt.

Der externe Zugangspunkt zum Netzwerk wurde deaktiviert und betroffene Server aus dem Netzwerk entfernt.

Es wurde kein Kontakt mit den Angreifern aufgenommen und auch keine Zahlung vorgenommen.

Unmittelbar wurden weiteren Absicherungsmaßnahmen vorgenommen und mit der Wiederherstellung der betroffenen Systeme begonnen.

Ein Zugriff auf Zugangsdaten zu Systemen und Kundenanlagen konnte in einem sehr eingeschränkten Bereich an diesem Tag nicht gänzlich ausgeschlossen werden. Da ein Großteil der Zugangsdaten in einem externen Password-Safe abgelegt sind, war der Bereich sehr eng begrenzt. Sicherheitshalber wurden trotzdem die Passwörter geändert.
Externe Services (wie Fernzugriffe), die für Kunden zur Verfügung gestellt sind, waren von dem Angriff nicht betroffen.

Dienstag, 2.4.2024

Ein Zugriff auf Zugangsdaten zu Systemen und Kundenanlagen war nur in einem sehr eingeschränkten Bereich möglich, da ein Großteil der Zugangsdaten in einem externen Password-Safe abgelegt sind. Zusätzlich wurden die Passwörter geändert.

Mittwoch, 3.4.2024

Die internen Services wurden weitgehend wiederhergestellt, sodass ein regulärer Betrieb am zweiten Arbeitstag wieder gegeben war.

Aus heutiger Sicht und nach Prüfung wurden keine Kunden – bzw. Lieferantendaten entwendet.

Donnerstag, 4.4.2024

Ein Spezialunternehmen der EDV Forensik wurde beauftragt um:

- Eventuell noch bestehende Lücken im Zugang von außen zu identifizieren
- Eventuell noch nicht erkannte Schadsoftware im System zu eruieren

Das Unternehmen hat den ersten Punkt bereits am Donnerstag abgeschlossen; erkannte Lücken wurden beseitigt.

Montag, 8.4.2024

Ergänzend zur erfolgten Absicherung des Zugangspunktes zu unserem Netzwerk arbeiten wir mit dem Forensik Unternehmen zusammen, um weitere Verbesserungen des Sicherheitskonzepts vorzunehmen.