Ransomware

Ransomware ist Schadsoftware, die Ihre Dateien verschlüsselt und damit unbrauchbar macht. Gegen "Lösegeld" bietet der Erpresser dann die Entschlüsselung an.
Überwindet der Schädling Ihre Schutzvorrichtungen (Virenscanner, Firewall, ...) und wird auf dem PC aktiv, sind potentiell alle Dateien auf diesem PC und in den Netzwerkfreigaben gefährdet.
Besonders hoher Schaden droht durch Zerstörung Ihrer IFW Datenbankdateien. Wird davon nur ein Teil verschlüsselt, werden alle Daten unbrauchbar. Eine vollständige Rekonstruktion ist nicht mehr möglich. Alle Eingaben seit der letzten Datensicherung sind verloren.
Es muss auf den Stand der letzten Datensicherung zurückgegangen werden.

Schutz der Dateien vor Ransomware

Es sind immer alle Dateien gefährdet, die ein User mit seinen Benutzerrechten verändern kann. Daher ist ein umfassender Schutz nicht möglich. Sie senken das Risiko wenn Sie keine Benutzer mit Administratorrechten für die tägliche Arbeit benutzen und täglich eine vollständige Datensicherung durchführen.

Schutz der IFW Datendateien vor Ransomware

Der Schutz der IFW Datenbankdateien kann signifikant erhöht werden, indem die Zugriffsrechte auf die IFW Datenbanktabellen über die Active Directory Verzeichnisrechte eingeschränkt werden. Dazu wird den Netzwerkusern das Recht Verzeichnisinhalte zu lesen (Ordner auflisten / Daten lesen) auf das IFW Verzeichnis entzogen.
Beachten Sie die folgenden Abschnitte und wenden Sie sich zur Umsetzung an Ihren Systembetreuer.

Schutz der Datensicherung vor Ransomware

Ransomware kann jede Datei zerstören auf die sie zugreifen kann. Je nach den Gegebenheiten können das auch die Dateien der Datensicherung sein. D.h., solange der Sicherungsdatenträger im Zugriff steht, gefährdet Ransomware auch die Sicherungsdateien:

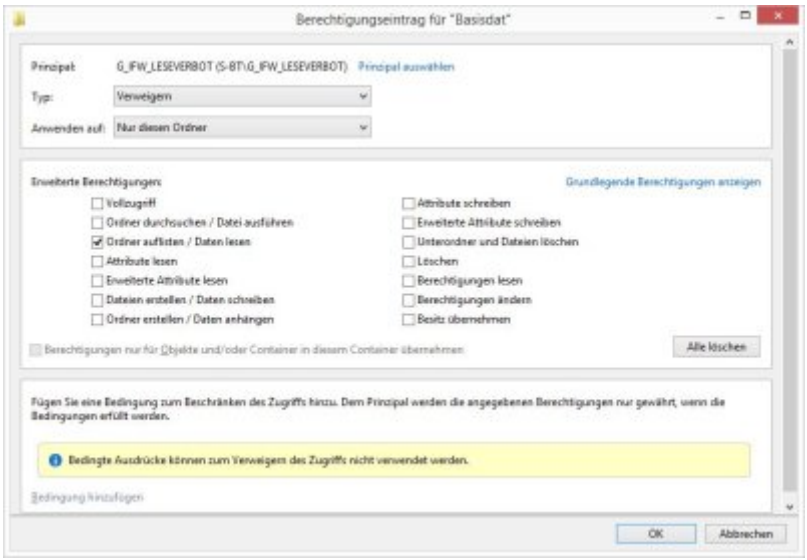
- normale User dürfen keinen Datenzugriff auf die Sicherungsdatenträger haben.
- Entfernen Sie den Sicherungsdatenträger möglichst kurz nach der Sicherung vom ausführenden Computer.
- Zur Aufbewahrung muss der Sicherungsdatenträger von der Hardware elektrisch getrennt sein.
- Sichern Sie auf wechselnde Datenträger, die sie täglich austauschen. So erhalten sie für für mehrere zurückliegende Tage jeweils eine Sicherung.
- Prüfen Sie täglich die Laufzeit, Datenmenge und Datum der Sicherung. Der Sicherungslauf kann auch "erfolgreich" melden ohne Daten gesichert zu haben.

Windows Benutzerrechte zum Schutz der IFW Datendateien vor Ransomware

Die folgenden Informationen sind für Systemadministratoren mit den entsprechenden

Sachkenntnissen:

- Erzeugen Sie im AD eine Gruppe IFW_LESEVERBOT.
- Erstellen Sie ein Verbotsrecht ("Verweigern") für die Gruppe IFW_LESEVERBOT. Verboten muss sein "Ordner auflisten / Daten lesen" und "nur diesen Ordner".



Wenden Sie es auf folgende Verzeichnisse:

zu sperrende Verzeichnisse	
IFW	Das IFW Rootverzeichnis
basisdat	das Verzeichnis mit den datenhaltenden Dateien
sysdat	das Verzeichnis mit Konfigurations-Dateien
IfwAblage	das Verzeichnis in dem das IFW Dateianhänge speichert. Ort variiert je nach Konfiguration. (Datei fakt.ini [Docustore])

je nach IFW installierten Zusatzmodulen sperren Sie weitere Ordner	
archfibu	Langzeitarchivierung von Finanzbuchhaltungsdaten (Zusatzmodul)
basisdat.???	Mandantenverzeichnisse 001 bis 999 (Zusatzmodul)
archiv	Langzeitarchivierung der Produktivdaten (Zusatzmodul)
archiv.???	Mandantenverzeichnisse 001 bis 999 (Zusatzmodul)
chgdat	Änderungsprotokoll (Zusatzmodul)
chgdat.???	Mandantenverzeichnisse 001 bis 999 (Zusatzmodul)

- Machen Sie alle normalen User zum Mitglied der Gruppe IFW_LESEVERBOT.
- Das Recht "Verweigern" hat Vorrang vor "Zulassen". D.h., der Admininistrator darf nicht Mitglied der Gruppe IFW_LESEVERBOT sein.
- **Der User, unter dem die Datensicherung ausgeführt wird, darf nicht Mitglied der Gruppe IFW_LESEVERBOT sein.**
- Anschließend sollten die Mitarbeiter den Inhalt der Verzeichnisse nicht mehr einsehen können.

Bitte beachten Sie:

- **Der Schutz wirkt nur, wenn die Mitarbeiter als Mitglied der Gruppe**

IFW_LESEVERBOT eingeloggt sind.

- Diese Maßnahme entbindet Sie nicht von der Notwendigkeit einer regelmäßigen, vollständigen Datensicherung. Die Datensicherung ist nach jedem Lauf auf Vollständigkeit und Korrektheit zu prüfen.
- Die neue Rechtestruktur schützt nur die IFW Dateien vor der Verschlüsselung. Andere Dateien wie z.B. Word Dokumente sind nicht geschützt.
- Nach einem Ransomwarebefall müssen ungeschützte Dateien aus der Sicherung restauriert werden.
- Das massenhaftes Kopieren der Datenbanktabellen als Mitglied der Gruppe IFW_LESEVERBOT ist nicht mehr möglich. Kopien für Laptops können so nicht mehr ausgeführt werden. Dazu muss ein separater User verwendet werden.
- Die IFW Administration wird erschwert. Ggf sollte ein IFWADMIN User eingerichtet werden.
- IFW Updates sind nur noch mit Admin rechten auf dem Server möglich.
- **Prüfen Sie nach der Umstellung, ob die IFW Datendateien weiterhin gesichert werden**.
- Stellen Sie sicher dass in Zukunft im Windows neu hinzugefügte Benutzer immer der Sperrgruppe (IFW_LESEVERBOT) zugeordnet werden.

Bei Fragen zum IFW setzen Sie sich mit uns telefonisch oder per Email (wruehle@ifw.de) in Verbindung.

Zur Erhöhung Ihrer Computersicherheit wenden Sie sich an Ihren Systembetreuer und berücksichtigen Sie die Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik.

From:
IFW Wiki - **www.wiki.ifw.de**

Permanent link:
https://wiki.ifw.de/wiki/doku.php?id=administratoren:schutz_vor_ransomware

Last update: **15.11.2022 11:40**