Leitfaden
Sicherer Umgang mit E-Mails

1 Hintergrund

Kriminelle versuchen immer wieder per Mail an Zugangsdaten zu gelangen oder Rechner mit Schadsoftware zu infizieren. Um das Vertrauen der Empfänger zu erlangen, werden E-Mail-Adressen bekannter Einrichtungen verwendet. Auch die Anschreiben werden immer wieder auf bestimmte Zielgruppen, wie zum Beispiel Personalabteilungen, zugeschnitten.

Neben dem Versuch, Zugangsdaten abzugreifen, werden verstärkt Anhänge verschickt, welche Schadcode enthalten. Dazu gehören auch Office-Dokumente, welche aktive Inhalte in Form von Makros enthalten können. Werden diese Makros aktiviert, beginnt der enthaltene Schadcode mit der Arbeit und verschlüsselt alle im Zugriff befindlichen Daten. Nach Abschluss der Verschlüsselung wird dem Nutzer/ der Nutzerin ein Erpressungsschreiben präsentiert, welches zur Zahlung eines Lösegeldes auffordert.

Virenscanner bieten in diesem Fall nur geringen bis gar keinen Schutz, da die Trojaner immer wieder verändert werden, um einer Erkennung zu entgehen.

Im folgenden wird aufgeführt, wie Infektionen vermieden werden können und was zu tun ist, wenn eine Infektion festgestellt wird.

2 Vermeidung von Infektionen

Generell ist beim Umgang mit E-Mails besondere Vorsicht geboten.

Erhalten Sie unaufgefordert E-Mails mit Anhängen, sollten die Anhänge auf keinen Fall geöffnet werden.

Auch wenn das Anschreiben und der Absender einer Mail legitim erscheinen, ist Vorsicht geboten, wenn in angehängten Office-Dokumenten zur Aktivierung von Inhalten aufgefordert wird.

Folgen Sie der Aufforderung zur Aktivierung von Inhalten in Office-Dokumenten generell nicht!

Wenn nötig, fordern Sie den Absender dazu auf, die Dokumente im PDF-Format zu schicken.
Schalten Sie das Ausführen von Makros im Trust Center von Excel, Word und Outlook ab.
https://www.uni-due.de/zim/locky-virus.php

Folgen Sie der Aufforderung, Zugangsdaten auf einer verlinkten Webseite einzugeben, nicht.

Fragen Sie Ihren IT-Ansprechpartner (PC-Betreuer, IT-Service-Center oder PC-Service), wenn Sie unsicher sind!

Fertigen Sie von all Ihren Daten regelmäßig Backups an!

Auch bei aller Vorsicht können Infektionen über Sicherheitslücken im Betriebssystem oder der eingesetzten Software auf Ihren PC gelangen. Daher bieten regelmäßige Backups den besten Schutz.

3 Infektionen erkennen und Gegenmaßnahmen

Sobald eine Infektion erfolgt ist, beginnt der Trojaner mit der Verschlüsselung.

Verschlüsselte Dateien sind in der Regel an einer veränderten Dateiendung, zum Beispiel „meineDatei.uDz2j8mv“ zu erkennen.

Nach Abschluss der Verschlüsselung startet der PC unaufgefordert neu, um auch den MBR der Festplatte zu verschlüsseln.

Schalten Sie in beiden Fällen den PC hart aus, indem Sie den Netzschalter am Netzteil betätigen und informieren Sie umgehend Ihren IT-Ansprechpartner (PC-Betreuer, IT-Service-Center oder PC-Service)!

Auch wenn sich Ihr PC ungewöhnlich verhält (z.B. langsame Reaktion auf Eingaben), kann dies ein Indiz für eine Infektion sein. Fragen Sie Ihren IT-Ansprechpartner!

4 Weitere Informationen

Das ZIM warnt regelmäßig in den RSS-Feeds vor aktuellen Bedrohungen.
https://www.uni-due.de/zim

Goldene Regeln - Sicherheitsgrundregeln für Arbeitsplatzrechner
https://www.uni-due.de/zim/services/sicherheit/goldene_regeln.shtml

Mailpolicy für die UDE
https://www.uni-due.de/zim/services/e-mail/mailpolicy.shtml

Ansprechpartner
https://www.uni-due.de/zim/soforthilfe/