Neue Welle von Verschlüsselungs- und Erpressungstrojanern

Dortmund, 15.06.2020: Beim Katholischen Datenschutzzentrum sind in den vergangenen Tagen mehrere Meldungen über Datenschutzverletzungen durch den Befall mit Schadsoftware eingegangen. Bei den uns gemeldeten Vorfällen handelt es sich um eine Schadsoftware, die sich im kompletten Netzwerk der betroffenen Einrichtung ausbreitet, in allen erreichbaren Verzeichnissen alle Dateien verschlüsselt und anschließend einen „Erpresserbrief“ z.B. als Textdatei hinterlässt, der zur Kontaktaufnahme mit den Kriminellen auffordert. Nicht nur die Benutzerdaten und E-Mail-Konten waren betroffen, sondern auch Backup-Dateien, die in vermeintlich „versteckten“ Bereichen des Dateisystems abgelegt waren. Gegen Zahlung eines „Lösegeldes“ wird die komplette Entschlüsselung der Dateien versprochen.

In der Regel dringt der Schädling über das Öffnen von infizierten Dateianhängen oder das Anklicken von Weblinks in E-Mails in die Netzwerke ein. Dazu werden zuvor durchaus echte und existierende E-Mail-Kontakte und E-Mail-Kommunikationen ausgespäht und abgefangen, um dann unter Nachbildung einer auf den ersten Blick plausibel erscheinenden E-Mail-Antwort den Empfänger zum Öffnen des präparierten Datei-Anhangs oder zum Aufruf des Web-Links aufzufordern. In einem weiteren Schritt wird dann weitere Schadsoftware, etwa ein Verschlüsselungsprogramm, nachgeladen.
Das Katholische Datenschutzzentrum empfiehlt allen kirchlichen Einrichtungen, ihre Mitarbeiter für die erneute Welle von Phishing-Mails zu sensibilisieren und die Hilfestellungen des Bundesamtes für Sicherheit in der Informationstechnik zur Vorbeugung eines Angriffs zu befolgen. Außerdem sollten die kirchlichen Einrichtungen diese Situation zum Anlass nehmen, die für den Schutz personenbezogener Daten notwendigen technischen und organisatorischen Schutzmaßnahmen auf ihre Wirksamkeit zu prüfen. Im Rahmen des ständigen Verbesserungsprozesses sollte auch geprüft werden, ob Schutzmaßnahmen anzupassen sind.

Bei der Eindämmung der Folgen eines Befalls mit Schadsoftware sind Backups ein sehr wichtiger Bestandteil. Um eine wirksame Option zur Widerherstellung der Daten sein zu können, sollte sichergestellt sein, dass die Backups für die Schadsoftware nicht auch über das Netzwerk der Einrichtung erreichbar sind, die Backups regelmäßig erstellt werden und dass diese auch Widerherstellbar sind. Auch dies sollte regelmäßig getestet werden.

Bei Entdeckung einer Schadsoftware sollten die IT-Verantwortlichen der Einrichtung unverzüglich gemäß den in der Einrichtung für solche Fälle vorhandenen Notfallplänen agieren. Die Polizei in NRW hat eine zentrale Stelle für die Bekämpfung der Cyber-Kriminalität eingerichtet, die in diesen Fällen ebenfalls weiterhelfen kann.