Notarin
Stephanie A. Jost

Notarin Jost ◦ Buchholzer Str. 32 ◦ 09456 Annaberg-Buchholz

Buchholzer Straße 32
09456 Annaberg-Buchholz

Fon (0 37 33) 14 03-0
Fax (0 37 33) 14 03-16

info@notarin-jost.de
www.notarin-jost.de

Mein Zeichen:	Ihr Zeichen:	Datum:
20762-sj		5. Januar 2021

Cyber-Angriff und Datenschutzvorfall

Sehr geehrte Beteiligte, Mandanten und Kunden,

leider wurde mein Notarbüro (Notarin Stephanie A. Jost) Opfer einer Schadsoftware. Dabei ist es nach derzeitigen Erkenntnissen leider nicht auszuschließen, dass die Angreifer (personenbezogene) Daten einsehen konnten, die sich ggf. auch auf Sie bzw. Ihr Unternehmen beziehen.

Was ist geschehen?

Am Dienstag, den 22.12.2020 wurde ein E-Mail-Anhang geöffnet. Der vermeintliche Absender war uns bekannt und eine Warnmeldung des von uns eingesetzten Virenscanners erfolgte nicht. Im weiteren Tagesverlauf erhielten wir mehrere Meldungen, dass nunmehr über unsere E-Mail-Adresse und in unserem Namen E-Mails verschickt werden, deren Anhang möglicherweise Schadsoftware enthält.

Daraufhin haben wir unter Mithilfe von IT-Sicherheits-Experten unsere Systeme sofort analysiert. Dabei wurde ein Befall mit der weitverbreiteten Schadsoftware Emotet festgestellt.

Was ist Emotet?

Emotet ist in der Lage, authentisch aussehende Spam-Mails zu verschicken, die dem Empfänger dazu verleitet, die sich im Anhang befindende Word/Excel-Datei zu öffnen. Die Schadsoftware liest Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Diese Information nutzen die Hacker zur weiteren Verbreitung des Schadprogramms in Spam-Kampagnen, so dass die Empfänger täuschend echte Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen.

Sobald ein Computer infiziert ist, können weitere Viren oder Trojaner eingeschleust werden, die ihre Zugangsdaten auslesen und vollständigen Remote-Zugriff auf das System ermöglichen.

Was haben wir gemacht?

Unverzüglich wurden alle erforderlichen Maßnahmen ergriffen, um die Schadsoftware zu eliminieren und die Sicherheit unserer Systeme wiederherzustellen. Sämtliche Systeme wurden vom Netz getrennt und ausführlich geprüft. Soweit erforderlich wurden Server und Clients neu aufgesetzt sowie mit neuen Passwörtern versehen.

Der Vorgang wurde bereits der zuständigen Datenschutzaufsichtsbehörde gemeldet.

Was können Sie tun, um sich zu schützen?

Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge von E-Mails (insbesondere Office-Dokumente, zumeist wird Emotet über .doc und .xml Anhänge verbreitet) und prüfen Sie in den Nachrichten enthaltene Links, bevor sie diese anklicken. Bei einer verdächtigen E-Mail sollten Sie im Zweifelsfall den Absender anrufen und sich nach der Glaubhaftigkeit des Inhaltes erkundigen.

Was können Sie tun, wenn Sie betroffen sind?

- Informieren Sie Ihr Umfeld über die Infektion, denn Ihre Mailkontakte sind in diesem Fall besonders gefährdet.
- Ändern Sie alle auf dem betroffenen Systemen (zum Beispiel im Web-Browser) gespeicherten und eingegebenen Zugangsdaten.
- Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor. Sollte Ihr Rechner mit Schadsoftware wie Emotet infiziert sein, dann empfiehlt es sich, diesen Rechner neu aufzusetzen.

Bitte entschuldigen Sie mögliche Unannehmlichkeiten.

Mit freundlichen Grüßen

Stephanie A. Jost