Sicherheit - E-Mail Konto || Phishing und Spam

Meine Freunde, Bekannte und Kollegen teilten mir mit, dass in meinem Namen merkwürdige Mails verschickt werden. Was kann ich tun?

Die Täter machen dies, um Schadsoftware oder schädliche Links zu verteilen. Die Täter hoffen, dass die Links oder Anhänge in den Mails angeklickt werden, da die Empfänger den Absender ja kennen. Viele Empfänger sind jedoch bereits sehr vorsichtig und sind über die ungewöhnlichen Mailinhalte irritiert, so dass diese nicht angeklickt werden. Einige fragten sogar beim echten Inhaber nach. Hier wird dann die Masche der Täter enttarnt.

Das Versenden solcher Mails kann mehrere Gründe haben:

Ihr E-Mail Konto ist noch in den Händen der Täter

Durch Schadsoftware, die auf Ihrem Computer ist oder durch Phishing sind die Zugangsdaten zu Ihrem E-Mail Konto in die Hände der Täter gelangt. Die Täter können diese Daten nun für den eigenen Versand einsetzen und ggf. sogar die Zugangsdaten so verändern, dass Sie selbst nicht mehr Zugriff haben.

Ihr E-Mail Konto war in den Händen der Täter

Ihre Daten wurden durch Schadsoftware oder Zugriff auf Ihren E-Mail Konto zu einem bestimmten Zeitpunkt abgegriffen. Dabei wurden auch die gespeicherten Kontakte mitgenommen, die nun mit den falschen Mails zu gespammt werden. Auch wenn alle Gegenmaßnahmen (z.B. Schadsoftwarebereinigung und Passwortänderung) vollzogen wurden, können die Täter die bereits mitgenommenen Daten weiterhin verwenden. Als Absender wird einfach weiterhin Ihre E-Mail-Adresse eingetragen. Dies können Sie leider auch zukünftig nicht verhindern.

Ihr Computer ist Teil eines Bot-Netzes

Schadsoftware auf Ihrem Computer kann auch dazu führen, dass Ihre Computer durch die Täter ferngesteuert wird. Ihr Computer wird zu einem sogenannten Bot-Rechner (von Roboter), der meist unerkannt im Hintergrund die Befehle der Täter ausführt. Das kann u.a. auch der Spamversand sein. Sie sind mit Ihrem Rechner jedoch nicht allein. Die Täter können massenhaft solcher Computer zu einem riesigen Bot-Netz zusammenschließen und diese vernetzte Kraft dann für illegale Zwecke missbrauchen. So sind auch Angriffe auf andere Computersystem keine Seltenheit.

Ihre E-Mail Adresse wurde anderweitig abgegriffen:

Falls Ihre E-Mail-Adresse anderweitig abgegriffen worden ist durch diverse Mailinglisten, öffentliche Bekanntmachung, ein Virus oder Phising Erfolg bei einem Verwandten, Kollgegen etc., kann ihr Name natürlich ebenso missbraucht werden. Dieser Missbrauch ist für die Täter dahingehend wichtig um vertrauen bei neuen Opfern aufzubauen und die Phising/Virus bzw. Spam-Attacke weiterzuverbreiten. Dies ist leider auch nicht zu verhindern. Man muss sich das ungefähr so vorstellen, als wenn man einen Brief schreibt und auf den Umschlag die falsche Absenderadresse schreibt.

Maßnahmen, die Sie ergreifen können:

Nutzen Sie ein aktuelles Antivirenprogramm und verwenden Sie zusätzlich den EU-Cleaner, den Sie auf www.botfrei.de kostenfrei laden können. Lassen Sie diese Softwarelösungen Ihren Computer ausführlich scannen. Dies kann je nach Datenmenge auch mehrere Stunden dauern. Drucken Sie die Reporte über Funde von Schadsoftware im Anschluss unbedingt aus. Notfalls erstellen Sie von diesem Protokoll einen Screenshot, den Sie ausdrucken können.

Ändern Sie Zugangsdaten und Passwörter aller genutzten Accounts. Achten Sie dabei darauf, dass eine Änderung von Passwörtern nur Sinn macht, wenn der Computer von Schadsoftware vollständig befreit ist und so keine neuen Daten erneut an die Täter gelangen. Einige Anbieter haben neben den Login Daten noch unterschiedliche Passwörter für den Mailversand.

Informieren Sie Ihre Kontakte über die mögliche Gefahr. Teilen Sie Ihren Bekannten mit, dass unbekannte Täter offensichtlich in Ihrem Namen Mails verschicken. Warnen Sie vor dem Öffnen von beigefügten Anhängen oder Links aus solchen Mails.

Melden Sie den Vorfall dem Rechenzentrum. Wenn Sie die Möglichkeit haben, senden Sie uns bitte die Reporte der Antivirenprogramme zu. Des Weiteren wären Beispiele der gesendeten Mails, die bei Ihren Bekannten eingegangen sind wichtig um den Header auswerten zu können. Wichtig dabei ist, dass der erweiterte Header/Briefkopf der E-Mails dabei ist. Dieser ist je nach E-Mail Dienst oder E-Mail-Programm unterschiedlich abzurufen.

Versuchen Sie sich daran zu erinnern, seit wann diese Mails verschickt werden und ob Sie in der Vergangenheit möglicherweise ungewöhnliches auf Ihrem Rechner bemerkt haben oder Sie auf eine Phishing E-Mail hereingefallen sind.

Prüfen Sie in Ihrem E-Mail Konto, ob dort Daten verändert wurden. So können zusätzliche Kontaktdaten (z.B. eine Weiterleitung Ihre Mails an eine zusätzliche Adresse) hinterlegt worden sein.

Prüfen Sie in Ihrem E-Mail-Konto, ob die Mails aus Ihrem Postfach verschickt wurden. Diese sind ggf. im "Gesendet"-Ordner noch vorhanden.

Prüfen Sie, ob die E-Mail-Adresse, die als Absenderadresse angegeben ist, mit Ihrer Adresse identisch ist. Immer wieder legen die Täter alternative Adressen an, die sich lediglich in der Endung z.B. .com unterscheiden. Ihre Kontakte bemerken diesen Unterschied ggf. nicht sofort.

Halten Sie Ihr Betriebssystem und Ihre Programme aktuell. Dadurch schließen Sie möglicher Sicherheitslücken, die von den Tätern ausgenutzt werden können.

Erstellen Sie Backups. Für den Notfall können Sie Daten wiederherstellen.

Sollte Schadsoftware vorhanden sein, so kann eine Neuinstallation des Betriebssystems ggf. der letzte Ausweg sein. Diese Schritte sind jedoch mit viel Aufwand verbunden.