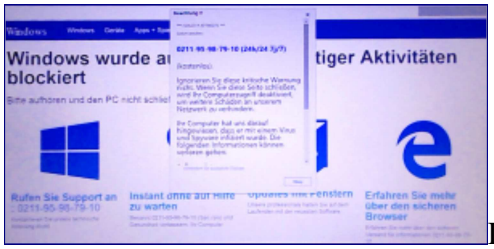
Diese zwei Betrugsversuche verunsichern ganz Deutschland

Wir möchten heute den Newsletter nutzen, um noch einmal eindringlich vor zwei Betrugsversuchen zu warnen, die derzeit wieder verstärkt in Deutschland die Runde machen. Über beide Fälle haben wir in den vergangenen Monaten bereits mehrfach berichtet. Dennoch erreichen uns zur Zeit jede Woche neue Anfragen von Menschen, die Opfer dieser Kriminellen wurden. Daher haben wir uns dazu entschieden, noch einmal die beiden Fälle zu schildern und zu erläutern, was zu tun ist, falls Sie selbst in diese Situation geraten. Die beiden Methoden können beschrieben werden als "**Der angebliche Microsoft-Anruf**" und "**Die angebliche Hacker-E-Mail**". Wir schreiben hier extra "angeblich", da beide Szenarien von den Betrügern frei erfunden sind: weder stammt der Anruf von einem echten Microsoft-Mitarbeiter, noch kommt die Mail von einem echten Hacker.

1. Der angebliche Microsoft-Anruf



Die Betrüger geben sich als Microsoft-Mitarbeiter aus und rufen auf dem Telefon zuhause an. In häufig schlechtem Englisch versuchen die Anrufer Ihnen zu erzählen, auf Ihrem Computer gäbe es ein Sicherheitsproblem und es müsse sofort gehandelt werden. Neuerdings verzichten die Betrüger auch auf den Anruf und blenden stattdessen Pop-up-Fenster auf Webseiten ein. Das heißt, man ist im Internet unterwegs und plötzlich öffnet sich ein neues Fenster, das alles andere überlagert (siehe Foto). Die Meldung, die erscheint,sieht aus, als ob der Windows-Computer selbst den Warnhinweis ausgeben würde.

Dabei handelt es sich aber eigentlich um eine klassische Werbeanzeige. Die Werbung ist nur so geschickt gestaltet, dass niemand merkt, dass es Werbung ist. Jeder Nutzer wird im ersten Augenblick denken, es sei eine Warnmeldung vom Windows-Computer. Die "kritische Warnung" behauptet, dass der Computer blockiert sei und weitere Schäden drohen, weil der Computer mit einem Virus infiziert sei. Oft wird auch behauptet, es müsse ein Sicherheitsupdate installiert werden, man solle schnell handeln. Doch Gottseidank, die Rettung sei nahe, es gebe eine schnelle Möglichkeit per Fernwartung, um den Computer sicher zu machen. Doch: Die "schlimmen angedrohten Konsequenzen" sind in Wahrheit völlig aus der Luft gegriffen, und wer auf die Fernwartung eingeht, ist in die Falle getappt. Gehen Sie auf diese Fernwartung ein, so erlangen die

Kriminellen vollen Zugriff auf Ihren Computer, können dort Änderungen vornehmen, Daten und Passwörter ausspionieren und Schadprogramme installieren. Danach verlangen die Betrüger für die angebliche Reparatur Ihres Computers sogar noch Geld.

Was ist zu tun?

Wenn Sie einen solchen Anruf erhalten sollten, **beenden Sie sofort das Gespräch und legen Sie auf**. Sind Sie auf den Betrugsversuch hereingefallen, dann sollten Sie die während des Betrugs installierte Software sofort entfernen, **alle (!) Kennwörter ändern und den PC mit einem Virenschutzprogramm untersuchen**. Ausserdem können Sie Ihr örtliches Polizeirevier kontaktieren und den Vorfall zur Anzeige bringen.

Microsoft nimmt dieses Problem sehr ernst und geht mit eigenen Ermittlern sowie in enger Zusammenarbeit mit Polizeibehörden weltweit gegen die Urheber dieser Betrügereien vor. Daher möchten wir Sie im Namen aller Betroffener bitten, den Fall auch auf der Internetseite von Microsoft zu melden, damit auch die Microsoft Digital Crimes Unit noch gezielter gegen diese Betrüger vorgehen kann. Den Link zu dem entsprechenden Formular finden Sie hier: http://support.microsoft.com/reportascam

2. Die angebliche Hacker-E-Mail

Die E-Mail, die in den letzten Wochen erneut für besonders große Aufregung gesorgt hat, ist unglaublich dreist. In der E-Mail behauptet der Absender ganz unverblümt, er hätte Ihren Computer gehackt. Doch damit nicht genug. Der angebliche Hacker behauptet weiter, er hätte zudem Ihre Kamera am Computer gehackt und Sie dabei gefilmt, wie Sie sich unseriöse Internetseiten angesehen hätten. Nun droht der Absender damit, diese Aufnahmen zu veröffentlichen und an alle Ihre Bekannten zu schicken, wenn Sie nicht einen bestimmten Betrag bezahlen. Die Mail endet also mit einer Erpressung.

Diese Mail kursiert in verschiedenen Versionen, zunächst nur auf Englisch, mittlerweile aber auch auf Deutsch. Die Mail hat vielen Menschen einen sehr großen Schrecken eingejagt, vermutlich weil die Vorgehensweise so neu ist. Noch nie zuvor hat in einer Spam-Mail ein Betrüger uns so direkt angeschrieben und behauptet, er hätte unseren Computer gehackt. Vermutlich aus diesem Grund wurde die Mail von vielen Menschen ernst genommen. Wir haben in den letzten Wochen immer wieder Zuschriften von Menschen erhalten, die uns fragten, was sie nun machen sollen.

Was ist zu tun?

Die Antwort ist hier einfach: Nichts! Sie müssen nichts tun, außer die Mail sofort zu löschen. Alles an dieser Mail ist frei erfunden! Egal wie abenteuerlich die Vorwürfe und Behauptungen klingen, lassen Sie sich bitte nicht davon verunsichern! Ignorieren Sie die Mail, löschen Sie sie und denken Sie nicht mehr darüber nach. Es ist einfach nur ein dreister Betrugsversuch, nichts weiter. **Ihr Computer wurde nicht gehackt, Ihre Kamera wurde nicht gekapert und es wurde auch kein Video von Ihnen gemacht.**

Diese Mail wurde auch nicht an Sie persönlich versendet, sondern millionenfach. Es bringt daher auch nichts, wie im obigen Fall, der ganz anders funktioniert, die Polizei zu informieren. Hier handelt es sich um eine herkömmliche Spam-Mail, die aus dem Ausland verschickt wird. Auch wir haben diese Mail schon mehrfach erhalten. Die Polizei kann hier kaum etwas unternehmen, der Absender ist kaum zu ermitteln.