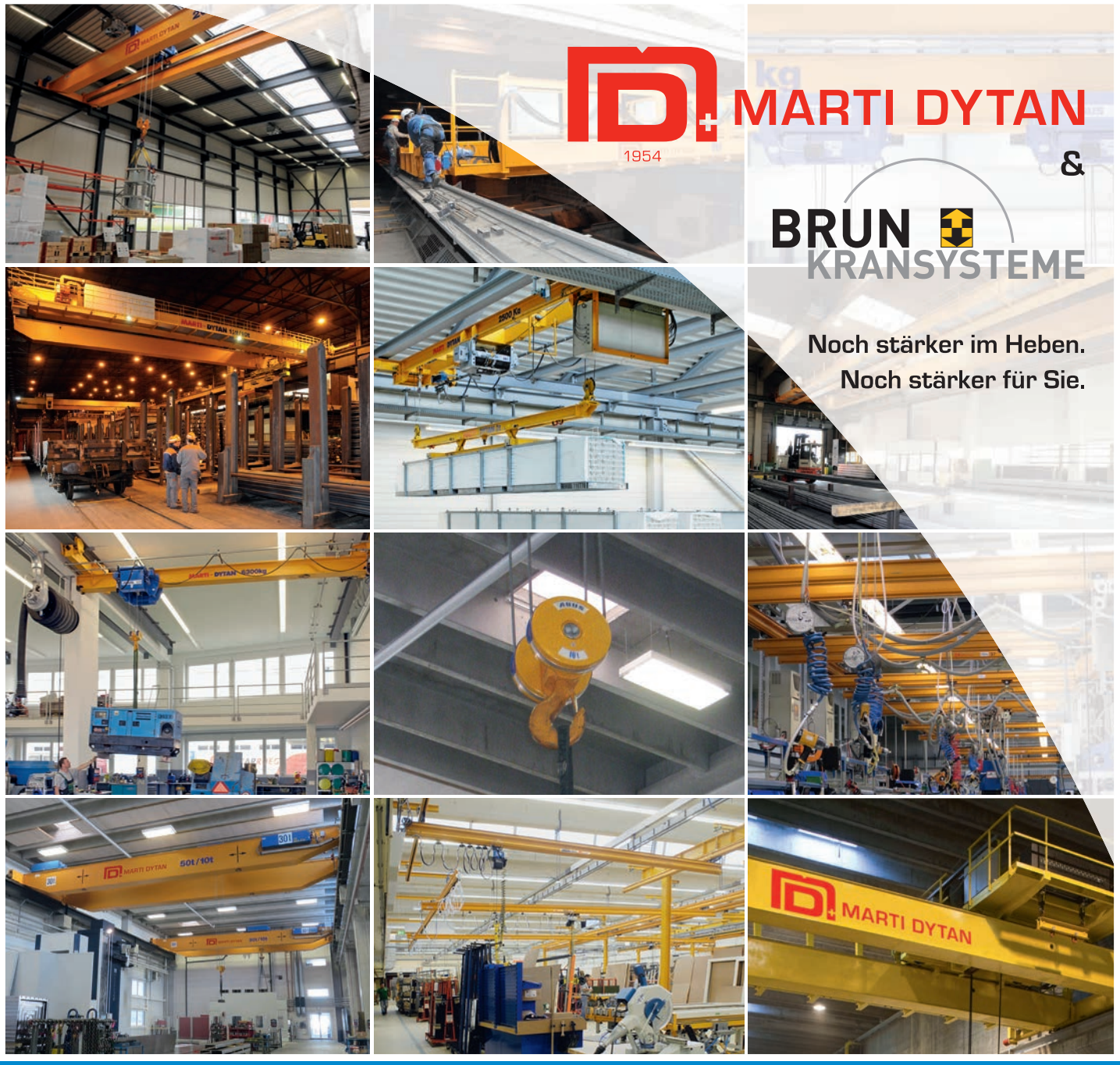
Das Schweizer Industriemagazin. Seit 1972.

Mit Schnell-zugriff

maschinenbau

Nr. 3 März 2016



Fishing – allgegenwärtig und gefährlich

In den vergangenen Wochen konnte viel über Fishing-Angriffe gelesen werden. Mittels mehr oder weniger trivialen E-Mails versuchen die Angreifer an persönliche Informationen, vor allem aber an Zugangsdaten und Passwörter zu gelangen.

Fishing, ein Kunstwort aus Password Harvesting Fishing, bezeichnet den Versuch an Benutzernamen, Codes, Passwörter oder andere vertrauliche Informationen zu kommen. Die Angriffsmöglichkeiten haben dabei verschiedene Gesichter. Oft werden dazu bekannte Firmen als Absender verwendet, mit dem Versuch, Vertrauen zu erwecken. Beispielsweise Credit Suisse als Absender, der Online-Banking-Account musste infolge eines Hackerangriffs gesperrt werden. Zum Reaktivieren müsse nur auf den untenstehenden Link geklickt werden. Oder ein weiteres Beispiel: DHL wollte ein Paket zustellen, da aber niemand zu Hause war, müsse nun ein Formular ausgefüllt werden, wann wieder jemand zu Hause ist und der DHL-Bote vorbeikommen könne. Bei beiden Angriffen ist grösste Vorsicht geboten. Immer wieder wird versucht, beim Aufruf der verlinkten Seite eine Malware (Virus, trojanisches Pferd oder dergleichen) zu installieren. Und dies auch, wenn das Formular gar nicht ausgefüllt wird. Daher gilt, diese E-Mails umgehend in den Papierkorb (Trash) zu verschieben.

Spuren werden unbewusst hinterlassen

Viele Menschen sehen sich nicht im Fokus eines Angriffs. «An meinen Daten hat eh niemand Interesse» oder «mit meinen Daten kann eh niemand etwas anfangen», sind Aussagen, die oft gemacht werden. Dies kann vielleicht stimmen, denn personenbezogene Angriffe sind (noch) eher die Ausnahme. Aber irgendwo in einem Gästebuch einen Eintrag mit der eigenen E-Mail-Adresse getätigt, an einem Wettbewerb mitgemacht oder auf der eigenen Homepage die E-Mail in uncodierter Form angebracht, und schon ist die E-Mail-Adresse auch für einen Angreifer sichtbar. Es gibt auch einen Handel mit diesen Adressen. Für wenige Dollar können im Internet tausende (gültige!) E-Mail-Adressen gekauft werden. Wer sich nun hinter einer der E-Mail-Adressen befindet, ist dabei unerheblich. Hauptsache, es wird auf den Link geklickt. Wenn von 1000 angeschriebenen Personen nur schon wenige auf diesen Angriff hereinfallen, kann sich dies bereits für einen Angreifer lohnen.

In der immer stärker vernetzten Welt hinterlässt jeder oft unbewusst seine Spuren. In den Nachrichten des Vereins wird von einem Wettkampf oder einem Anlass erzählt und die Personen mit Namen veröffentlicht. Diese dann mit Facebook, Xing, Twitter oder dergleichen kombinieren und viele Informationen über einen Menschen kommen zusammen. Yasni.ch ist eine spezialisierte Personensuchmaschine, aber Vorsicht beim Besuch der Seite! Besuchen Sie diese nur mit einem aktuellen gepatchten Betriebssystem und aktuellem Antivirenprogramm. Auf dieser Seite können Informationen über eine Person auf einfachstem Weg gesucht werden. Einfach den Namen eingeben und einen Moment warten. Die Suchmaschine durchsucht verschiedene andere Seiten und stellt alle Antworten übersichtlich dar. Diese Informationen können anschliessend für einen personenbezogenen Angriff verwendet werden.

Leser in die Irre führen

Der aktuelle 21. MELANI-Halbjahresbericht (Melde- und Analysestelle Informationssicherung, www.melani.admin.ch) vom 29. Oktober 2015 zeigt, dass Fishing nach wie vor ein grosses Thema ist. Praktisch täglich stellen die Mitarbeiter mehr oder weniger grossflächige Fishing-Kampagnen fest.

Dabei sind es weiterhin oft triviale Angriffe wie gefälschte Steuerformulare, E-Mails von Banken, aber auch aktuelle Themen wie die Flüchtlingsproblematik versuchen den Leser in die Irre zu führen. Jedoch sind auch immer mehr professionelle E-Mails dazu gekommen. Die Anrede ist nicht mehr Pauschal oder enthält nur die E-Mail-Adresse, sondern der Leser wird korrekt mit Vor- und Nachnamen angesprochen. Dies soll das Vertrauen in die E-Mail verstärken. Auch der Autor hat einige solcher E-Mails erhalten. Bei einigen musste auch er mehrmals darauf

Bild: Archiv

Es gibt einen Handel mit E-Mail-Adressen.

ZUM AUTOR

Andreas Wisler
goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.gosecurity.ch
wisler@gosecurity.ch

Das wird angezeigt.

http://www.hier-geht-es-hin.ch/

schauen, um den Fishing-Angriff zu erkennen. Im geschäftlichen Umfeld könnte die E-Mail beispielsweise vom Chef kommen, mit der Bitte eine spezielle Seite zu besuchen, im privaten Umfeld von einer ehemaligen Schulkollegin, die man schon lange nicht mehr gesehen hat. Werden in der E-Mail Dinge erwähnt, die eigentlich niemand anderes kennen kann, ist das Misstrauen bereits viel geringer und der Versuch auf den Link zu klicken nicht mehr so weit entfernt.

Ein Klick kann reichen

Um die Mitarbeiter auf solche Gefahren zu sensibilisieren, kann ein gezielter Fishing-Angriff durchgeführt werden. Ein Szenario könnte zum Beispiel wie folgt ablaufen:

1. E-Mail im Namen des Geschäftsführers mit der Bitte, an einer Umfrage zur Erhöhung der Informationssicherheit mitzumachen.
2. Beim Klick erscheint eine Webseite, die genau im Design der Firmenseite erstellt wurde. Darin befinden sich einige Fragen zum Umgang mit dem Passwort (Länge, Änderungsrhythmus, Aufgeschrieben, Jemandem mitgeteilt usw.). Am Ende der Umfrage befindet sich ein Feld zur Kontrolle der Passwortstärke. Ein Balken von Rot nach Grün zeigt, ob das Passwort wirklich sicher ist, oder nicht. Fett steht der Hinweis «wird nicht gespeichert».
3. Beim Absenden werden alle Angaben an den Server geschickt, inklusive dem eingegebenen Passwort.

Die Auswertungen von über einem Dutzend durchgeführten Angriffen zeigt ein ernüchterndes Bild. Obschon immer wieder von Fishing gelesen werden kann, klicken über zwei Drittel der angeschriebenen Personen auf den Link. Etwa die Hälfte der Personen füllt auch das Formular aus. Wäre dies ein echter Angriff gewesen, wäre das Firmenkennwort in die falschen Hände gelangt. Doch schon der Klick auf den Link könnte, wie bereits erwähnt, reichen, den Firmen-Rechner mit einer Malware zu verseuchen. Die Auswertung der Zugriffe zeigt, dass die benutzten Geräte (installierter Browser und enthaltene Plugins) oft nicht auf einem aktuellen Patchstand sind und so leicht missbraucht werden können.

Wie können Sie sich vor Fishing-E-Mails schützen?

- Geben Sie nie persönliche Informationen preis
  Kein seriöser Dienstleister wird seine Kunden jemals per E-Mail-Nachricht oder Telefon zur Angabe von Passwörtern oder Kreditkartendaten auffordern.
- Geben Sie die Internetadressen nach Möglichkeit manuell ein oder überprüfen Sie diese vor einem Klick darauf. Nachfolgendes Beispiel zeigt, was angezeigt wird und wohin der Link wirklich führt:
  Gerne werden auch Schreibfehler oder Buchstabendreher für solche Angriffe verwendet. Auch könnte die Erweiterung falsch sein (.com anstelle .ch).
- Misstrauen Sie E-Mails, die Sie unaufgefordert bekommen. Besonders vertrauenswürdige Firmen werden gerne als gefälschte Absender-Adressen missbraucht. Dabei werden auch Schweizer Firmen für gezielte Fishing-Angriffe auf Schweizer E-Mail-Adressen verwendet. Bekannte Firmen für solche Angriffe in den vergangenen Monaten waren Swisscom, das Bundesamt für Energie oder Läderach Schokolade, um nur mal drei zu nennen.
- Seien Sie vorsichtig, wenn Sie E-Mails bekommen, die eine Aktion von Ihnen verlangen und ansonsten mit Konsequenzen (Geldverlust, Strafanzeige, Konto- oder Kartensperrung, verpasste Chance, Unglück) drohen.
- Verschiedene Firmen bieten ein Formular oder eine E-Mail-Adresse an, mit welchen ein Fishingangriff gemeldet werden kann.

Vorsicht walten lassen

Zugenommen haben auch Fishing-Angriffe per Telefon. Dabei wird versucht, den Angerufenen auf eine Webseite zu locken oder persönliche Informationen preis zu geben. Gerade angebliche Anrufe vom Microsoft-Support (oft in Englisch) verunsichern den Windows-Nutzer. Die Betrüger rufen wahllos Haushalte an und verlangen, dass auf dem Computer des Angerufenen dringend eine Sicherheitssoftware installiert werden müsse, da der Support einen Fehler beziehungsweise einen Schädling festgestellt hat. In einem zweiten Schritt werden dann Zugangsdaten oder die Kreditkartennummer abgefragt.

Mit all diesen Angriffen wird versucht, an die Hilfsbereitschaft oder an die Ängstlichkeit der angeschriebenen Personen zu appellieren. Da immer wieder Personen auf diese Art von Angriffen hereinfallen, hören diese auch nicht auf, sondern nehmen nur zu. Es ist wichtig, bei seltsamen E-Mails Vorsicht walten zu lassen. Lieber einmal zu viel eine E-Mail löschen, als auf einen Angriff hereinfallen. Mit gesunder Skepsis können viele Angriffe erkannt und erfolgreich verhindert werden.

Anzeige