9. April 2020

Sehr geehrte geschätzte Ingram Micro Partner,

Wir möchten Sie darauf aufmerksam machen, dass sich betrügerische Verkaufsaufträge im Umlauf befinden. Als Distributor unternehmen wir alles in unserer Macht Stehende, um dieses Verhalten einzudämmen und um uns selbst, unsere Hersteller und unsere Kunden zu schützen.

Bitte achten Sie genau auf Details und verdächtige Aktivitäten! Uns wurden Betrugsfälle bei unseren Partnern, deren langjährigen Kunden (deren E-Mail-Adressen missbraucht wurden) wie auch von "neuen Kunden", bekannt, die zu 100% betrügerisch sind.

Um Ihnen zu helfen, Betrug zu erkennen und zu stoppen, bieten unsere Ingram Micro-Verkaufsteams großartige Beratung an.

Für neue Kunden
Wenn eine Bestellung von einem neuen Kunden eingeht, unaufgefordert ist und zu schön erscheint, um wahr zu sein, dann ist sie es wahrscheinlich auch. Andere potenzielle Betrugssignale, sind

- Wenn der neue Kunde unter Zeitdruck steht und mit jedem Preis, den Sie ihm geben, einverstanden ist.
- Wenn der Kunde etwas bestellt, das nicht zu Ihrem Kernbereich gehört (Speicher, Laptops, Tablets).
- Wenn der neue Kunde möchte, dass Sie über Nacht eine große Bestellung ohne Rücksicht auf die Kosten aufgeben.
- Wenn Sie eine betrügerische Bestellung eines Neukunden vermuten, was sollten Sie tun?
- Führen Sie eine Internetsuche nach dem Firmennamen durch und vergleichen Sie die E-Mail-Adresse mit der bekannten Firmendomain.
- Kontrollieren Sie mit Google Earth jede Adresse, die Ihnen als "Lieferadresse" gegeben wurde, und sehen Sie sich die Standorte und ihre Umgebung an. Lagerhäuser in trostlosen Gegenden oder nicht näher beschriebene Büroparks und Spediteur-Adressen sind für Betrüger gängige Lieferadressen.
- Überprüfen Sie alle Adressen für diese Firma im Internet und bestätigen Sie, ob die Adresse, an die sie Sie liefern lassen, eine davon ist. Seien Sie gewarnt - Betrüger sind dafür bekannt, dass sie Straßennummern oder Postleitzahlen an ihrem Lieferort so umstellen, dass sie den tatsächlichen Adressen der Endbenutzer sehr ähnlich sehen.

Für bestehende Kunden
Auch Ihre bestehenden Kunden können das Ziel von Betrügern werden. Die Betrüger dringen in ihre E-Mail-Systeme ein und erstellen PO's auf dem Briefkopf des Unternehmens, die völlig legitim aussehen können - insbesondere, wenn sie direkt von einer gültigen E-Mail-Adresse eines bekannten Kunden verschickt werden. Achten Sie auf anormale Käufe. Ist es der von Ihnen verwaltete Security-Client mit 50 Mitarbeitern, der Ihnen eine Bestellung für 150 Laptops schickt?
Was sollten Sie tun, wenn Sie eine betrügerische Bestellung von einem bestehenden Kunden vermuten?

- Überprüfen Sie die Ihnen für den Antrag zugesandte E-Mail-Adresse sorgfältig. Bei einem üblichen Trick wird bei E-Mail-Adressen ein Zeichen vom eigentlichen Firmen- oder Unternehmensdomain-Namen geändert oder ein .net anstelle von .com oder .org verwendet.
- Prüfen Sie, ob sich der Lieferort von dem Ort unterscheidet, an den Sie normalerweise liefern (z.B.: ein anderer Staat, eine völlig andere Adresse oder eine unwahrscheinliche Adresse für dieses Unternehmen oder diese Dienststelle).

9. April 2020

- Führen Sie eine Internetsuche durch und vergleichen Sie die Domain-Website mit der Domain-E-Mail-Adresse.
- Nehmen Sie den Telefonhörer in die Hand - und rufen Sie Ihren Kunden zur Überprüfung an.
- Machen Sie eine schnelle Bestandsaufnahme. Wenn der bestehende Kunde ein ungewöhnliches Produkt UND in ziemlich außergewöhnlichen Mengen kauft, rufen Sie ihn über die Telefonnummer an, die SIE für ihn gespeichert haben, und nicht über die, die in der Ihnen mit der Anfrage zugesandten E-Mail steht.

Betrug ist nicht mehr so leicht zu erkennen wie früher. Die Betrüger werden immer besser und raffinierter. Bei Ingram Micro schulen wir unser Team kontinuierlich, um potenzielle Betrüger zu erkennen und Sie im Zweifelsfall direkt zu kontaktieren.

Lassen Sie uns gemeinsam betrügerische Bestellungen eliminieren.

Herzliche Grüße,

Eric Kohl
Vizepräsident, Advanced Solutions
Ingram Micro Inc.