DIGITAL SKIMMING

EUROPOL EC3 European Cybercrime Centre

WAT IS HET?

Een grote cybersecurity dreiging

Digital skimming is het onderscheppen van betaal- en transactiegegevens van klanten tijdens een online betaling.

De transactiegegevens worden onderschept tijdens de betaalhandeling. Dit gebeurt zonder dat de klant daar weet van heeft.

Vormen van digital skimming

Digital skimming aanvallen worden ook wel web skimming, online card skimming, e-skimming, formjacking of **Magecart** genoemd.

Magento is een open source e-commerce platform waar digital skimming activiteiten als eerste op werden gericht. Hier komt ook de naam **Magecart** vandaan, als combinatie van 'Magento' en 'shopping cart', deze naam verwijst ook naar de criminele groep achter de aanvallen.

HOE GAAT HET IN ZIJN WERK?

Over het algemeen kunnen er drie stappen worden onderscheiden bij een digital skimming aanval:

Het verkrijgen van toegang
Criminelen krijgen toegang tot de code of server van een online winkel, of tot de code van een derde partij.
Dit kan plaatsvinden door kwetsbaarheden, configuratiefouten of door middel van een bruteforce aanval.

Het invoegen van code
Malware wordt geplaast in de betaalketen.

Het onderscheppen en verzamelen
Klant- en betaalgegevens worden onderschept. Deze data kan direct worden verzonden naar criminelen of verhuld worden opgeslagen op de server voor latere verzameling.

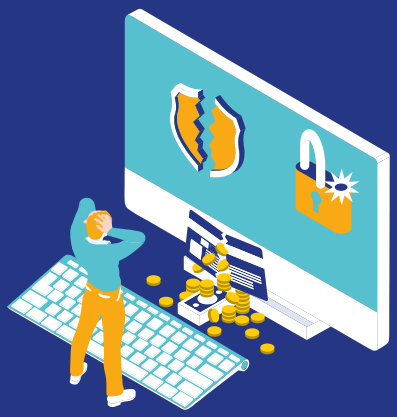
De klanten zien dat hun bestelling succesvol wordt afgerond en dat de bestelling wordt ontvangen.
Zij zijn zich hierdoor niet bewust van het feit dat hun gegevens zijn buitgemaakt.

DIGITAL SKIMMING

EUROPOL
EC3 | European Cybercrime Centre

WAAROM IS DIT BELANGRIJK?

Er is een toename van het aantal digital skimming aanvallen.
En de aanvallen kunnen soms lang onopgemerkt blijven waardoor er potentieel van erg veel klanten gegevens worden buitgemaakt.
Wanneer een aanval wordt opgemerkt heeft dat impact op niet alleen de betrouwbaarheid van de betreffende webshop, maar ook in de veiligheid van het online betalingsverkeer in het algemeen.



WAT KUNT U DOEN OM UW WEBSHOP TE BESCHERMEN?

De volgende acties dragen bij aan het beperken van digital skimming:

Maak gebruik van monitorings- en detectiesoftware om de aanwezigheid van malware te signaleren.

Het periodiek (laten) uitvoeren van een audit op de beveiliging en op kwetsbaarheden van het betreffende e-commerce platform van de webshop en op gebruikte derde partij software binnen het platform.

Zorg voor het tijdig toepassen van beveiligingsupdates en (kritische) software updates.

Zorg voor het toepassen van 2-factor authenticatie en een goed wachtwoordbeleid voor werknemers of externen die toegang hebben.

Voorzie uw medewerkers van training en bewustwording op het gebied van spearphishing aanvallen.

Beperk de toegang tot het beheer van de webshop door bijvoorbeeld enkel bekende IP- adressen en locaties.

Voer Content Security Policy (CSP) en Subresource Integrity (SRI) maatregelen door. Deze beperken de mogelijkheden om code te laten invoegen in de webshop.

WAT TE DOEN ALS UW WEBSHOP IS GERAAKT?

- Reset direct alle accounts van beheerders en databases na een malware infectie.
- Gebruik een malware scanner om malware te vinden.
- Gebruik een malware scanner om backdoors te vinden die mogelijk zijn geïnstalleerd om zich weer toegang te verschaffen.
- Verzamel alle beschikbare informatie met betrekking tot de aanval en het advies is om aangifte te doen bij de politie.
- Bij een lek van persoonsgegevens, of wanneer u het vermoeden heeft dat dit heeft plaatsgevonden, neemt u binnen 72 uur contact op met de autoriteit persoonsgegevens om hier melding van te maken.