Veilig Online

Mijn Reis Naar Digitale Beveiliging

Veilig Online

Mijn Reis Naar Digitale Beveiliging

Marc Huyghebaert

Schrijver: Marc Huyghebaert
Coverontwerp: Brave New Books - Nederland
ISBN: 9789465013350

Uitgave versie : Eerste druk , versie Maart 2024
Gedrukt door: Brave New Books - Nederland

D I S C L A I M E R

Alle foto's in dit boek blijven eigendom van hun respectievelijke makers en mogen niet worden gereproduceerd, gekopieerd of gebruikt zonder hun uitdrukkelijke toestemming.

De genoemde merknamen zijn eigendom van hun respectieve bedrijven. We hebben geen banden met deze bedrijven, tenzij uitdrukkelijk vermeld.

Het is belangrijk om te begrijpen dat dit boek bedoeld is als een leidraad en niet als een exacte wetenschap. Hoewel het waardevolle inzichten en informatie biedt over cyberveiligheid, biedt het op zichzelf geen garantie of bescherming tegen mogelijke cyberbedreigingen.
Het is aan de lezer om deze informatie te gebruiken als onderdeel van een bredere strategie voor cyberveiligheid, die regelmatig moet worden geëvalueerd en aangepast om rekening te houden met veranderende bedreigingen en risico's.
We raden lezers dan ook aan om professioneel advies in te winnen en hun eigen onderzoek te doen voordat ze beveiligingsmaatregelen implementeren.

DANKWOORD

Graag wil ik mijn dankbaarheid uitspreken aan iedereen die de tijd heeft genomen om mijn teksten na te lezen, tests uit te voeren en mij te inspireren, moed te geven, kracht te bieden en te steunen op momenten waarop ik het gevoel had dat ik niet verder kon. Jullie steun heeft mij geholpen om door te zetten en het beste uit mezelf te halen.

Het is niet altijd gemakkelijk om een project of doel te bereiken en ik ben me ervan bewust dat ik dit niet alleen had kunnen doen. De steun en feedback die ik heb ontvangen hebben mij geholpen om mijn werk te verbeteren en te groeien als persoon.

Ik realiseer me ook dat het niet vanzelfsprekend is dat mensen hun tijd en energie steken in de ondersteuning van anderen. Ik waardeer het daarom des te meer dat er mensen zijn die dat wel doen. Jullie hebben mijn leven verrijkt en ik zal jullie steun nooit vergeten.

Nogmaals, hartelijk dank voor jullie steun en aanmoediging. Ik zal deze ervaring koesteren en als motivatie gebruiken voor toekomstige uitdagingen en doelen die ik wil bereiken.

VOORWOORD

Het doel van dit verzamelboek is om u een waardevol instrument en handvat te bieden, waarmee u uw online veiligheid kunt waarborgen en beschermen.

Cybersecurity is een complexe uitdaging en er zijn veel factoren die afzonderlijk of gezamenlijk uw veiligheid in gevaar kunnen brengen. Dit verzamelboek biedt inzicht in de belangrijkste bedreigingen en risico's waarmee u online te maken kunt krijgen en geeft praktische adviezen en oplossingen om deze risico's te verminderen.

Om uw cybersecurity verder te verbeteren, bieden wij op maat gemaakte trainingen aan. Onze trainingen zijn gericht op het vergroten van uw bewustzijn van de gevaren van het internet en op het aanleren van effectieve technieken en ‘best practices’ om uzelf te beschermen. We begrijpen dat elke persoon en elk bedrijf anders is en daarom bieden we trainingen die speciaal zijn afgestemd op uw individuele behoeften en eisen.

Onze toewijding ligt bij het verbeteren van uw online veiligheid en het voorzien van de nodige tools en kennis om veilig te blijven in de digitale wereld. Wij begrijpen dat het belangrijk is om op de hoogte te blijven van de nieuwste technieken en bedreigingen, en daarom bieden wij voortdurend actuele informatie en trainingen aan om u te helpen. Onze missie is om u te ondersteunen bij het creëren van een veilige online omgeving voor uzelf, uw gezin en/of uw bedrijf.

Als men een schoendoos neemt, dan is de grootte ervan bekend. Bij Cybersecurity en hacking is er echter geen grootte of vast einde. Ieder moment van de dag komt er wel iets nieuws bij. Voor mij persoonlijk gaat het erom de computergebruiker bewust te maken van de gevaren van het internet.

Dagelijks horen we in het nieuws over mensen die in de val zijn getrapt. En nu komt iets wat velen niet graag zullen horen, maar meestal is het hun eigen schuld of hebben ze (onbewust) mee bijgedragen aan de oplichting of inbreuk. Onbewust, maar het had voorkomen kunnen worden.

Ik ga dus proberen om zoveel mogelijk technische en juridische zaken uit te leggen. In onze Cybersecurity Awareness Trainingen kunnen wij u effectief laten zien hoe Phishing werkt, hoe men uw pc, gsm, camera of microfoon kan overnemen, enzovoort.
Hoe dit precies in zijn werk gaat, hoeft u niet in dit boek te verwachten. Dit is geen handleiding voor aspirant-hackers, laten we dat duidelijk stellen.
Iets leren en kunnen is één ding, het vertellen en tonen gaat nog wel, maar het op papier zetten is totaal iets anders. We gaan dus ons best doen.

Veel leesplezier!

BIO

Mijn naam is Marc Huyghebaert. Ik behaalde mijn eerste certificaat voor ethisch hacken in augustus 2021, gevolgd door mijn Bachelor in Security Management in december van datzelfde jaar.

Een essentieel aspect van Security Management is hacking en ik blijf mezelf voortdurend bijscholen door het volgen van cursussen. Mijn doel is om mensen van alle leeftijden bewust te maken van het belang van cybersecurity en in het bijzonder van hacking. Het internet kan namelijk een gevaarlijke plek zijn en het is belangrijk dat mensen zich bewust zijn van de mogelijke risico's en gevaren.

Als cybersecurity-professional wil ik mensen laten zien hoe criminelen hen kunnen aanvallen en vooral hoe ze zichzelf kunnen beschermen tegen deze bedreigingen. Door het vergroten van het bewustzijn en het delen van mijn kennis en expertise hoop ik bij te dragen aan een veiligere digitale wereld voor ons allemaal.

Inhoudstafel

Het internet

Het internet is een wereldwijd netwerk van computers dat informatie en gegevens met elkaar deelt. Het werkt op basis van een reeks protocollen en technologieën die ervoor zorgen dat computers over de hele wereld met elkaar kunnen communiceren.

Om te beginnen hebben we de basisbouwstenen van het internet: computers. Computers zijn apparaten die zijn uitgerust met speciale software en hardware om verbinding te maken met het internet. Elke computer die is verbonden met het internet, wordt een "host" genoemd.

Het internet maakt gebruik van een communicatieprotocol dat bekend staat als het Internet Protocol (IP). Elke computer die is verbonden met het internet heeft een uniek IP-adres, dat fungeert als een soort digitaal identificatienummer. Dit IP-adres maakt het mogelijk voor computers om elkaar te vinden en informatie uit te wisselen.

Wanneer een computer gegevens wil verzenden naar een andere computer op het internet, wordt de informatie opgedeeld in kleine pakketjes. Elk pakketje bevat de bron- en doel-IP-adressen, evenals een deel van de gegevens. Deze pakketjes worden via het internet naar hun bestemming gestuurd.

Om ervoor te zorgen dat de pakketjes de juiste bestemming bereiken, wordt gebruikgemaakt van routers. Routers zijn speciale computers die de pakketjes doorsturen naar andere routers totdat ze uiteindelijk hun bestemming bereiken. Routers gebruiken complexe algoritmen en tabellen om te bepalen waar de pakketjes naartoe moeten worden gestuurd om de meest efficiënte route te vinden.

Een ander belangrijk aspect van het internet is het Domain Name System (DNS). Aangezien IP-adressen niet erg gemakkelijk te onthouden zijn, wordt het DNS gebruikt om namen van websites om te zetten naar IP-adressen. Wanneer je bijvoorbeeld een website wilt bezoeken, typ je de domeinnaam in je webbrowser. De browser vraagt vervolgens het IP-adres van die domeinnaam op bij een DNS-server, waardoor de browser de juiste IP-adressen kan vinden en de website kan openen.

Om ervoor te zorgen dat gegevens veilig worden verzonden over het internet, wordt gebruikgemaakt van beveiligingsprotocollen zoals SSL (Secure Sockets Layer) of zijn opvolger TLS (Transport Layer Security). Deze protocollen versleutelen de gegevens tijdens de overdracht, waardoor het moeilijk wordt voor kwaadwillende om de gegevens te onderscheppen of te lezen.

Ten slotte, om inhoud op het internet te hosten en toegankelijk te maken, worden servers gebruikt. Servers zijn krachtige computers die speciale software draaien om webpagina's, bestanden en andere inhoud op te slaan en te leveren aan gebruikers die erom vragen.

Samengevat maakt het internet gebruik van een combinatie van computers, protocollen, routers, DNS en servers om informatie over de hele wereld te verzenden en toegankelijk te maken. Het is een complex systeem dat ons in staat stelt om te communiceren, informatie op te zoeken, te delen en te genieten van een breed scala aan online diensten en mogelijkheden.
Het begint allemaal met een IP-adres.

Wat is een IP-adres? Waarom is het nodig, maar ook potentieel gevaarlijk? Wat is een DNS-server? Wat is een domeinnaam? We zullen deze vragen beantwoorden hier proberen zo eenvoudig mogelijk te beantwoorden.

Een diepgaande blik op IP-adressen:

Het Ontstaan, Het Verschil tussen IPv4 en IPv6, en Interne en Externe IP-adressen

Introductie:

In de huidige digitale wereld is het begrijpen van IP-adressen essentieel. Of je nu een fervente internetgebruiker bent of een professional in de IT-sector, kennis van IP- adressen helpt je de fundamenten van het internet te begrijpen. In dit artikel zullen we een diepgaande blik werpen op IP-adressen, hun ontstaan, het verschil tussen IPv4 en IPv6, en het onderscheid tussen interne en externe IP-adressen.

Het Ontstaan van IP-adressen:

IP-adressen zijn ontstaan als een systeem om unieke identificatie toe te wijzen aan elk apparaat dat is verbonden met een computernetwerk. In de beginjaren van het internet, werd het Internet Protocol versie 4 (IPv4) geïntroduceerd. IPv4-adressen bestaan uit vier reeksen cijfers, gescheiden door punten. Elke reeks kan variëren van 0 tot 255, waardoor er ongeveer 4,3 miljard unieke IPv4-adressen beschikbaar zijn.

Vergelijk een IP-adres met uw huisnummer die een adres heeft, een identificatiemiddel voor elk apparaat dat verbonden is met internet. Wanneer je een apparaat met je router verbindt, via een kabel of wifi, krijgt dat apparaat automatisch een uniek IP-adres toegewezen binnen uw netwerk, door de router. Dit zijn de interne IP-adressen.

Daarnaast krijgt elke router die verbonden is met internet een extern IP-adres toegewezen, dit gebeurt door de internet provider.

Het Verschil tussen IPv4 en IPv6:

Met de exponentiële groei van internetgebruik en de toenemende behoefte aan meer unieke IP-adressen, kwam IPv4 op een punt waarop de beschikbare adressen bijna waren uitgeput. Dit leidde tot de ontwikkeling van het Internet Protocol versie 6 (IPv6). In tegenstelling tot IPv4, bestaat een IPv6-adres uit acht groepen van vier hexadecimale cijfers, gescheiden door dubbele punten. Dit resulteert in een enorme toename van het aantal beschikbare IP-adressen, met een totaal van ongeveer 340 undeciljoen (3,4 × 10^38) adressen.

Interne IP-adressen:

Interne IP-adressen worden gebruikt binnen een lokaal netwerk (Local Area Network of LAN). Ze dienen om apparaten binnen het netwerk te identificeren en communicatie tussen deze apparaten mogelijk te maken. Bij een typisch thuisnetwerk worden interne IP-adressen toegewezen door de router via het Dynamic Host Configuration Protocol (DHCP). De meest voorkomende reeks interne IP-adressen is 192.168.0.0 tot 192.168.255.255, waarbij het derde en vierde octet variabel zijn.

Interne IP-adressen zijn bedoeld om te identificeren met welk specifiek apparaat uw router communiceert. In het voorbeeld xxx.xxx.x(xx).x(xx), houdt de notatie in dat de derde en vierde groep cijfers niet noodzakelijk uit drie cijfers hoeven te bestaan.

IP-adressen die beginnen met 192.xxx.x(xx).x(xx) zijn interne adressen binnen jouw LAN-netwerk, dus achter jouw router. Bijvoorbeeld, 192.168.0.1 is een intern IP-adres dat door je router wordt toegewezen. Het kan dus voorkomen dat je buurman in zijn LAN ook hetzelfde IP-adres toegewezen krijgt.

Het belangrijkste om te onthouden is dat een IP-adres dat begint met 192.xxx.x(xx).x(xx) een intern IP-adres is, specifiek voor jouw netwerk. Er kunnen en er mogen zelfs geen 2 toestellen met hetzelfde ip adres verbonden zijn met uw router, want dan weet deze niet meer met wie de router een het communiceren is.

“Router” is het bakje aan de muur die u van uw internetprovider kreeg.

“Lan” is uw intern thuis netwerk, dit kan volledig uit een wifi netwerk bestaan, of een mix met toestellen verbonden met een kabel.

Externe IP-adressen:

Externe IP-adressen worden gebruikt voor communicatie tussen het lokale netwerk en externe netwerken, zoals het internet. Een externe IP-adres wordt toegewezen aan de router of het modem dat het lokale netwerk met het internet verbindt. Dit adres fungeert als een unieke identificatie voor het netwerk op het internet. Internetproviders kunnen dynamische of statische externe IP-adressen toewijzen aan gebruikers, afhankelijk van het type internetabonnement. Het externe IP adres is dus verbonden met uw fysieke locatie, uw huis of kantoor in de meeste gevallen.

In het kort samengevat

IP-adressen vormen de ruggengraat van het internet en zijn cruciaal voor het mogelijk maken van communicatie tussen apparaten en netwerken. Het ontstaan van IP-adressen begon met IPv4, dat vier reeksen cijfers gebruikte en ongeveer 4,3 miljard unieke adressen bood. Met de groeiende behoefte aan meer adressen en de introductie van IPv6 met zijn acht reeksen hexadecimale cijfers, werd het aantal beschikbare adressen drastisch vergroot naar een duizelingwekkend aantal.