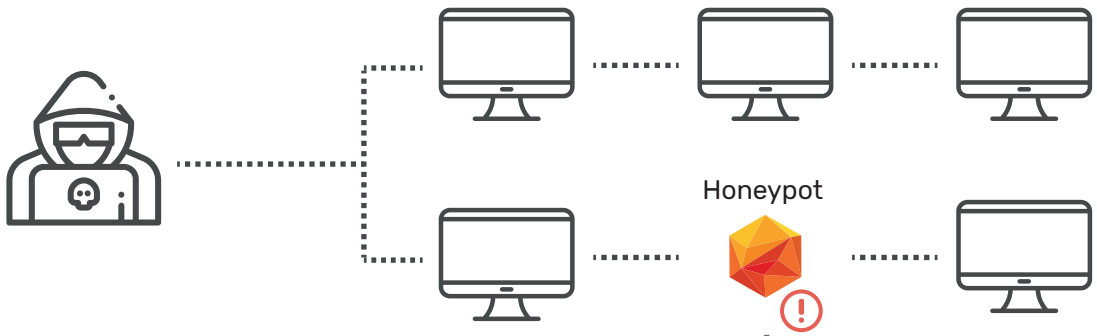
SECURITYHIVE

Honeypot Software voor bedrijven die Cyber Security serieus nemen

NL #1
Criminele cyber hotspot van Europa

20%
Van het MKB heeft last van cyber crime

191
Dagen totdat een hack is geïdentificeerd



Direct op de hoogte wanneer het er het meest toe doet.

Ieder jaar ontdekken vele bedrijven dat ze gehackt zijn of te maken hebben met een datalek. Gemiddeld genomen hebben hackers 191 dagen vrij spel tot deze hacks en datalekken worden ontdekt, als ze al worden ontdekt. Zelfs bedrijven die duizenden euro's uitgeven aan digitale veiligheid, hebben geen idee of er momenteel een hacker aanwezig is op het netwerk.

Met de SecurityHive Honeypot Software bent u snel op de hoogte van een hack of datalek. Hackers zullen na binnenkomst op het netwerk op onderzoek uitgaan. Komt de hacker uw Honeypot tegen? Dan brengt de Honeypot u direct op de hoogte.

De Honeypot verzamelt informatie die u in kunt zetten tijdens het opstarten van forensisch onderzoek.

De Honeypot creëert bewustzijn binnen de organisatie over de actuele veiligheidsrisico's.

Door de informatie van de Honepyot kan u uw beveiligingsmaatregelen evalueren en optimaliseren.

SECURITYHIVE

Hoe werkt onze Honeypot?

Onze Honeypot is een fysiek of virtueel netwerkapparaat dat zich voordoet als een legitiem apparaat in uw netwerk. Denk hierbij aan bijvoorbeeld een computer, server of VoIP-telefoon. De Honeypot kan zo ingesteld worden dat deze naadloos aansluit op uw bedrijfsnetwerk.

Na het instellen van de Honeypot hoeft u enkel te wachten tot de Honeypot een aanvaller of malware detecteert. Er is geen ruimte voor twijfel. Wanneer de Honeypot kwaadaardig netwerkverkeer detecteert is dit altijd verkeer dat niets te zoeken heeft op de Honeypot. Bij een detectie wordt u direct op de hoogte gebracht via email, Slack en/of SMS.

U heeft mogelijk al een probleem, u weet het alleen nog niet. De Honeypot van SecurityHive verandert dat!

Ik heb een Firewall, heb ik dan ook een Honeypot nodig?

Jazeker! De firewall is de eerste stap naar een veiliger netwerk. De Honeypot mag hierin eigenlijk niet ontbreken. Een Firewall doet immers niets meer dan netwerkverkeer wel of niet doorlaten naar zijn bestemming.

Hierdoor kan er een vals gevoel van veiligheid onstaan. U heeft uw voordeur beveiligd met een Firewall, maar de hackers komen via de achterdeur nog eenvoudig binnen. Door het plaatsen van Honeypots in uw netwerk heeft u altijd een bewegingssensor actief, waar een Firewall enkel rekening houdt met de voordeur.

Vormt een Honeypot een extra veiligheidsrisico?

Nee, de Honeypot zal geen extra veiligheidsrisico opleveren voor uw netwerk.
Er zijn diverse maatregelen getroffen die ervoor zorgen dat een implementatie in uw netwerk zo veilig mogelijk kan worden uitgevoerd. Zo hebben wij ervoor gezorgd dat; wij nooit contact op kunnen nemen met de Honeypot; de software is uitgevoerd in geïsoleerde containers; een hacker niet uit de Honeypot kan breken; de Honeypot niet gebruikt kan worden om aanvallen naar andere systemen uit te voeren.

Wat als een aanvaller de Honeypot hackt of DDOS't?

De Honeypot is ervoor gemaakt om misbruikt te worden door aanvallers. Wanneer de Honeypot wordt aangevallen, zal deze altijd een melding versturen naar uw dashboard welke wordt gehost op de beveiligde servers van SecurityHive. Wat daarna met de Honeypot gebeurt maakt niet zoveel uit, omdat de Honeypot niets van waarde opslaat en u al een melding heeft ontvangen.

Wat als een aanvaller achterhaalt dat er een Honeypot actief is? Werken ze hier dan niet omheen?

Om te kunnen achterhalen dat er een Honeypot actief is, zal de aanvaller actief verbinding moeten maken met de Honeypot. Wanneer dit gedaan wordt, heeft de Honeypot zijn primaire functie al vervuld, namelijk; een melding maken van ongeauthoriseerd netwerkverkeer op de Honeypot.

U zult dus altijd een melding ontvangen van een verbindingspoging, zo bent u op direct op de hoogte van een cyberaanval.