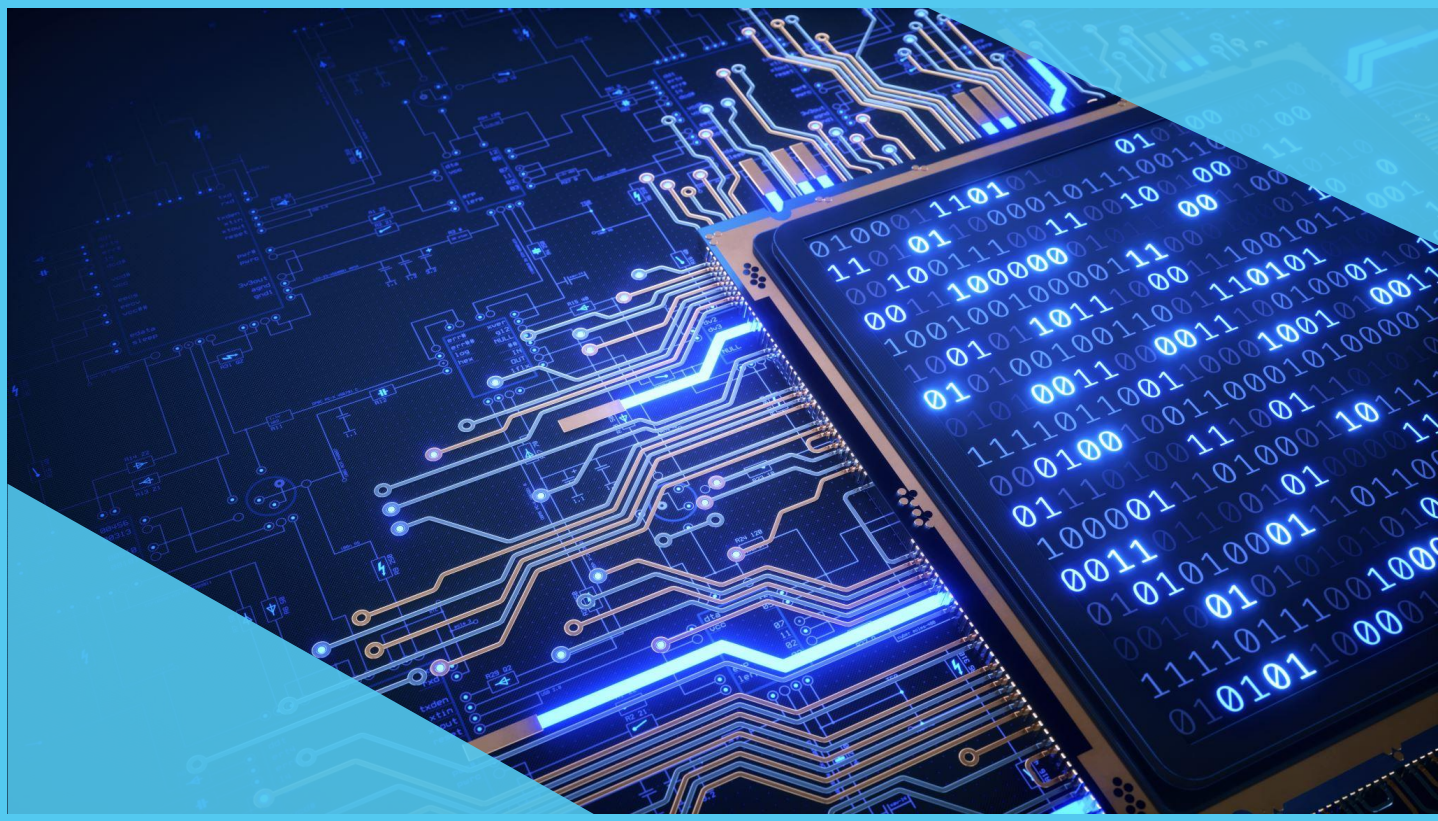
Samen aan de slag met

SECURITY

RESOLVIT



2024

SECURITY WHITEPAPER

Trends & ontwikkelingen – Security baselines – Quick wins

Eindhoven www.resolvit.nl info@resolvit.nl +31 (0)40 30 30 370

Samen aan de slag met

SECURITY

Cyberaanvallen worden steeds geavanceerder

Wat als een cyberaanvaller niet jouw bedrijf, maar een van jouw klanten wil aanvallen, en dat doet via jouw e-mailsysteem en later blijkt dat jij je security niet op orde hebt? Of wat als een cyberaanvaller klantdata weet te stelen en dreigt dit publiekelijk te delen als er geen losgeld wordt betaald?

Eén op de vijf bedrijven krijgt te maken met een cyberaanval, waarbij de gemiddelde schadepost oploopt tot drie à vier ton. Sommige bedrijven denken dat ze niet interessant genoeg zijn voor hackers, echter schetsen bovenstaande voorbeelden een ander beeld. Door jouw data te encrypten, of dreigen data publiekelijk te delen, kan een hacker jouw bedrijfsprocessen volledig stilleggen of zorgen voor imagoschade.

Hoe kun je ervoor zorgen dat jouw bedrijf dit niet overkomt? Helaas, de oplossing om 100% veilig te zijn bestaat simpelweg niet. Wel kunnen we door samen te werken aan jouw digitale veiligheid de kans op een succesvolle cyberaanval zo klein mogelijk maken.

+300% Ransomware aanvallen afgelopen jaar, met meer dan 50% gericht op MKB bedrijven

1 in 4 Bijna één op de vier MKB bedrijven zegt het afgelopen jaar een datalek te hebben gehad

95% van de hacks komt door menselijke fouten

Cyberaanvallen worden ieder jaar geavanceerder

€300K Gemiddelde schadepost is gestegen van €184K naar €300K

De kans op een brand is 1:8.000, de kans op een inbraak is 1:250 en de kans op een cyberaanval is 1:5.

RESOLVIT

Samen aan de slag met

SECURITY

Belangrijke trends in het land van cybersecurity

Generative AI (GenAI) in Cybersecurity: GenAI-technologieën, zoals grote taalmodellen, zijn een dubbelzijdig zwaard in cybersecurity. Aan de ene kant bieden ze krachtige tools voor dreigingsdetectie en respons, maar aan de andere kant kunnen ze ook door cybercriminelen worden gebruikt om geavanceerde malware te ontwikkelen. Het is cruciaal dat je je bewust bent van de potentie van GenAI om zowel de verdediging te versterken als de aanvalsmogelijkheden van tegenstanders te vergroten.

Zero Trust Beveiliging: De manier van hoe we IT gebruiken is veel verandert, jouw securitystrategie moet dat dus ook. Zero Trust is een beveiligingsconcept dat ervan uitgaat dat geen enkele gebruiker of systeem wordt vertrouwd zonder verificatie. Deze benadering wordt steeds belangrijker als een manier om zowel interne als externe bedreigingen te minimaliseren.

Wachtwoordloze Authenticatie: De verschuiving naar wachtwoordloze authenticatiemethoden, zoals biometrie en passkeys, is een trend die naar verwachting zal doorzetten in 2024. Deze methoden bieden een hoger niveau van beveiliging en gebruiksgemak.

Strengere Regelgeving: Er komen steeds meer regelgevingen om de digitale veiligheid te waarborgen. De nieuwe Cybersecurity Regulation van de EU, die in januari 2024 in werking is getreden. Ook komt de NIS2-richtlijn, voluit de Network and Information Security directive, eraan. Deze richtlijn introduceert strengere eisen en breidt de reikwijdte uit naar nieuwe sectoren1. Onder NIS2 moeten bedrijven en organisaties adequate maatregelen nemen op gebieden zoals cyberrisicobeheer, penetratietesten, incident response en herstel. Niet-naleving kan leiden tot financiële sancties die gebaseerd zijn op de wereldwijde omzet van bedrijven.

Tips & quick wins

GenAI geeft hackers de mogelijkheid om meer en betere phising content te creëren dan ooit te voren.

Verhoog de security awareness van medewerkers zodat ze weten waar ze op moeten letten.

De nieuwe manier van (hybride) werken brengt nieuwe security uitdagingen met zich mee. Leer wat Zero Trust kan betekenen voor jouw organisatie.
Zero Trust Guidance Center | Microsoft Learn

De meeste hacks vinden nog altijd plaats door zwakke wachtwoorden. Ga zonder wachtwoord te werk.
Implementing Passwordless Authentication with Microsoft Entra ID for SMB - Part 1 (youtube.com)

Regelgeving zoals NIS2 gaat een flinke impact hebben op veel bedrijven. Bekijk welke impact dit heeft op jouw bedrijf en welke stappen je alvast kunt nemen.
Samenvatting NIS2-richtlijn | Over het NCSC | Nationaal Cyber Security Centrum

Hulp nodig?
info@resolvit.nl
+31 (0)40 30 30 370

RESOLVIT

Samen aan de slag met

SECURITY

In de dynamische wereld van cybersecurity is het essentieel om niet alleen te reageren op dreigingen, maar ook proactief te handelen. Goede security policies vormen de ruggengraat van een robuuste verdediging tegen de steeds veranderende aard van cyberaanvallen.

Onze aanpak is gebaseerd op drie verschillende security baselines, die elk ontworpen zijn om onze klanten te beschermen tegen een breed scala aan dreigingen. Van fundamentele netwerkbeveiliging tot geavanceerde bedreigingsdetectie en respons, onze baselines bieden een gelaagde verdediging die essentieel is in het huidige digitale landschap.

Laten we samen de reis beginnen naar een veiligere toekomst, waarbij we de kracht van preventie, detectie en respons combineren om een veiligheidsnetwerk te creëren dat net zo dynamisch is als de aanvallers die we tegenkomen.

Resolvit Baseline

BASIC

Ons Basic niveau biedt essentiële beveiliging voor jouw dagelijkse online activiteiten. Met real-time monitoring op werktijden, antivirusbescherming en firewallbeheer, houdt je de basisbedreigingen buiten de deur.

- Min. Microsoft Secure Score 70%
- Multi-factor authenticatie

Resolvit Baseline+

ADVANCED

Het Advanced niveau tilt je beveiliging naar een hoger plan met geavanceerde dreigingsdetectie en versleutelde datacommunicatie. Ideaal voor bedrijven die hun cyberbeveiliging willen versterken zonder de complexiteit.

- Min. Microsoft Secure Score 80%
- Managed Detection & Respons
- Security Awareness

Resolvit Baseline++

EXPERT

Kan jouw productie voor geen moment stil komen te liggen? Kies dan voor de ultieme bescherming met een volledig pakket van geavanceerde beveiligingsmaatregelen. Dit omvat op maat gemaakte oplossingen en 24/7 respons op incidenten zodat je altijd een stap voor bent op de cyberdreigingen.

- Min. Microsoft Secure Score 90%
- Data labeling
- Uitgebreid security assessment

RESOLVIT

Samen aan de slag met

SECURITY

Krijg vertrouwen in de cyberweerbaarheid van jouw organisatie

Door samen met Resolvit aan de slag te gaan met het verhogen van jouw securitylevel krijg je vertrouwen in de cyberweerbaarheid van jouw organisatie. We begrijpen dat niet iedereen op Enterpriselevel digitaal beveiligd hoeft te worden, en dat er altijd een balans moet worden gevonden tussen gebruiksvriendelijkheid en mate van security. Gebruikers moeten immers altijd goed hun werk kunnen doen.

Securityverbeteringen kunnen vaak het beste stapsgewijs worden uitgevoerd. Na de inventarisatie kunnen we gezamenlijk bepalen welke elementen de meeste prioriteit hebben en dit verwerken in een security planning. Onze security dienstverlening kan, net zoals de Moderne Werkplek, worden afgenomen o.b.v. een maandelijkse te betalen abonnement zodat er geen investering vooraf benodigd is en je direct van start kunt met optimaliseren.

www.resolvit.nl @ info@resolvit.nl +31 (0)40 30 30 370

RESOLVIT