TESORION

Software zit in steeds meer apparaten en steeds meer van die apparaten zijn **verbonden met internet**. Dat is riskant, want software heeft vaak **zwakke plekken**. Cybercriminelen maken daar graag **misbruik** van. Weet je waar die zwakke plekken zitten? En hoe ga je daarmee om?

Weet je sowieso wel van alle apparaten op je netwerk welke software-versies ze draaien? En of dat ook de nieuwste versies zijn? Dat allemaal bijhouden is voor een gewoon bedrijf niet te doen. Daarom doen wij het voor je. Want wat gebeurt er als je je software niet update? Dan zet je een deur open voor cybercriminaliteit. Beveiliging is een race tussen de leverancier en de criminelen.

“Hè nee, weer een software update! Dat komt nu echt niet uit. Net nu ik voor een deadline zit. Laat die update maar even wachten, dat kan ook straks wel.” Je medewerker heeft geen tijd voor deze onderbreking van zijn werk. Maar de volgende dag zit er een hacker op het bedrijfsnetwerk. Hoe kwam die binnen? Toch via deze laptop.

Inzicht in urgentie

Onze scans geven je een totaalbeeld van kwetsbare systemen plus een trendanalyse van alle kwetsbaarheden in je infrastructuur. Alles in één helder overzicht.

Bovendien laten wij je zien wat de meest urgente gevallen zijn. Dat doen we op basis van de ernst van de kwetsbaarheid: is er bijvoorbeeld malware voor in omloop? Maar we kijken ook naar het belang van het apparaat voor je bedrijfsvoering.

Effectief risicomanagement

Welke systemen scannen we voor je? Webapplicaties (lokaal en in de cloud), firewalls, endpoint-beveiliging, plug-ins en nog veel meer meer. Kortom: je hele IT-landschap.

Dat geeft je de controle die je nodig hebt voor effectief risicomanagement. Je kunt bewuste, weloverwogen keuzes maken. Daarmee kun je ook voldoen aan ISO- en NEN-normen. Want die eisen dat beveiliging geen improvisatie is, maar doordacht beleid.

Continu bewaking

Cybercriminelen zijn continu op zoek naar inkomsten. Dat doen zij door geautomatiseerd te scannen naar systemen die kwetsbaar zijn.

Updates komen immers niet allemaal tegelijk, en soms staan apparaten uit. De situatie verandert dus voortdurend. Dat vraagt om constante waakzaamheid. Tesorion gaat min of meer op dezelfde wijze op zoek naar deze kwetsbaarheden binnen jouw netwerk.

Met het verschil om jou inzicht te geven in deze kwetsbaarheden zodat je een cyberincident kan voorkomen.

TESORION

Fokkerstraat 4
3833 LD Leusden

T: +31 33 456 3663
E: sales@tesorion.com

www.tesorion.com

Tesorion 7 checklist

De basis op orde. Waar begin je als jij je wilt wapenen tegen cybercriminelen?

1. Maak **medewerkers** weerbaar
We weten dat we niet op dat linkje moeten klikken. Ook weten we dat we niet zomaar geld moeten overmaken. Toch letten we niet altijd even goed op en trappen we er misschien allemaal wel eens in.

2. Splits je **netwerk** op in **compartimenten**
Segmenteer je netwerk. Zie het als brandwerende compartimenten. Wanneer er brand in een bepaald deel is kan je de branddeur sluiten en gaat niet het hele pand verloren.

3. Beveilig apparaten, e-mail en social media
We werken overal waar we willen. E-mail is in veel organisaties het belangrijkste communicatiemedium. Daarom wil je direct kunnen ingrijpen op apparaten die vreemd gedrag vertonen of zijn geïnfecteerd.

4. Versleutel belangrijke data
Data is het nieuwe goud, waarom beschermen we het dan niet net zo? Zorg dat je belangrijke data versleuteld bewaart, zodat wanneer data op straat komt te liggen deze niet toegankelijk is voor derden.

5. Maak betrouwbare **back-ups**
Het maken van back-ups lijkt een open deur. Back-ups zijn belangrijk, zo niet essentieel, om binnen afzienbare tijd (deels) verder te kunnen werken in geval van bijvoorbeeld ransomware.

6. Regel **toegang** tot bedrijfsmiddelen
Alle medewerkers hebben ongetwijfeld een eigen gebruikersnaam en wachtwoord. Waarschijnlijk heb je ook al sterke authenticatie ingeschakeld. Alleen een wachtwoord is niet veilig genoeg.

7. Houd je software en apparaten **up-to-date**
Overal zit tegenwoordig software in. Er zijn legio voorbeelden van software die kwetsbaarheden bevatten. Juist hierdoor kunnen cybercriminelen binnenkomen. Kortom: hoe ga jij om met deze updates?

24/7 actief
180+ experts
500+ klanten
1.000+ sensoren
4+ mln beschermde apparaten
100% Europees

ISO/IEC 27001 Information Security Management · NEN 7510 Information Security in Healthcare
EUROPOL The No More Ransom Project · EC3 European Cybercrime Centre