Perfect Day

CYBER ADVIES

JE CYBEREXPERT

Thomas Mes

thomas@perfectday.nl

085-048 61 09

ALSJEBLIEFT,

Hier zijn de resultaten van de Cyber Scan. Het geeft je een goed beeld van de digitale veiligheid van Bouw Groep. Complimenten, je hebt de Noodprocedure en Ketenveiligheid al grotendeels op orde. Als het gaat om de Operationele Techniek, Medewerkers en AVG adviseer ik je aan de slag te gaan. Je doet dit snel en makkelijk door ons security pakket af te sluiten. Daarmee pak je direct de meest voorkomende risico's aan. De bevindingen en aanbevelingen in dit rapport zijn gebaseerd op de informatie die ik heb gekregen uit de afspraak op kantoor met Jan Parel op 1 juli en het telefonische overleg met Robert van der Kraft van ABC-ICT.

Dit is een voorbeeldrapport. Het genoemde bedrijf, de namen en de adviezen zijn fictief. De eindscores komen in dit rapport ook niet overeen met de adviezen en zijn ter indicatie. Het rapport beschrijft in hoofdlijnen de risico's in de bedrijfsprocessen, in het gedrag van medewerkers en in de techniek. Het geeft ook weer in hoeverre je aan de wet- en regelgeving omtrent gegevensbescherming voldoet.

In een echte scan bespreken we veel meer punten, gaan we dieper op de zaken in en scannen we ook de e-mail en de website. We bekijken dan ook zaken zoals restoretests, het updatebeleid, monitoring, MDM, veilige softwareontwikkeling, server redundantie, VPN, veilig werken in de cloud, MFA, bewaartermijnen, het betaalproces, awareness onder de medewerkers, BYOD, toegangsbeveiliging en meer.

CYBERADVIES

SCORE

Je ziet hier de overall score van het bedrijf per thema. De uitwerkingen en aanbevelingen per thema vind je op de volgende pagina's.

MEDEWERKERS

Je kunt nog veel verbeteren aan het bewustzijn en veiligheid van medewerkers, met name in de productiehal. Denk daarbij aan algemene awareness, wachtwoordbeleid en 2FA.

TECHNIEK

De techniek op het kantoor (IT) is grotendeels op orde, echter in de productiehal (OT) niet. Daar zijn belangrijke verbeteringen nodig, met name segmentatie van het netwerk, back-ups en veilige (API)koppelingen.

WETGEVING

De AVG is deels op orde. Kijk nog naar de benodigde registers en sluit met alle partijen een verwerkersovereenkomst af. Zet jullie privacyverklaring op de website.

NOODPROCES

De medewerkers weten welke leveranciers ze moeten bereiken bij een cyber incident, ook als het gaat om de operationele techniek (OT). Er is een bellijst met noodnummers en een plan voor een datalek.

KETENVEILIGHEID

Er is inzicht in de ketenveiligheid. Met de leveranciers en afnemers zijn (onderhouds)contracten afgesloten. De impact op het productieproces bij een cyber incident is niet bekend. Voer een risicoanalyse uit.

ADVIES

ACTIELIJST

Hieronder volgt de lijst met praktische actiepunten. Deze lijst is geordend van meest kritiek tot voor verbetering vatbaar. Aan het eind van het rapport vind je standaard adviezen om de beveiliging te verbeteren.

MEDEWERKERS

Creëer meer awareness onder de medewerkers op de werkvloer.

KRITIEK: 90% van de hacks en datalekken ontstaat door onvoorzichtigheid van medewerkers. Door de medewerkers te trainen op het herkennen van een verdachte mail, link of bestand verklein je de kans dat je bedrijf slachtoffer wordt van cybercriminelen. Spookfacturen en phishing e-mails zijn steeds moeilijker te herkennen omdat er veel aandacht aan de opmaak en de inhoud wordt besteed. Vaak zijn ze persoonlijk gericht en vanuit een bekend adres gestuurd en daardoor moeilijk van echt te onderscheiden.

Het bewustzijn rond de cybersecurity van de medewerkers op de werkvloer is niet hoog. Jullie hebben onlangs een ransomwareaanval gehad die door middel van phishing tot stand is gekomen. Meerdere medewerkers hebben op de phishinglink geklikt en daardoor is malware op het netwerk terecht gekomen. Hierdoor hebben de productielijnen langere tijd stil gelegen. Creëer meer awareness door de cybersecurity en de privacy regelmatig met alle medewerkers te bespreken, bijvoorbeeld tijdens het bedrijfs- of teamoverleg. Controleer bij twijfel altijd de afzenders en de links in de e-mail door er eerst met de muis overheen te bewegen voordat jullie er op klikken. Zo zien jullie waar de link naar toe verwijst. Wees ook alert op de bijlage in de e-mail en scan deze eerst. Stel hier eventueel een beleid voor op en communiceer dit met alle medewerkers. Volg een (online) training op het gebied van cyber security en de privacywet, zodat iedereen hiervan op de hoogte is en blijft, en jullie de kans op hacks, ransomware of andere cyberaanvallen verkleinen.

TECHNIEK

Leg voor productie (OT) en kantoor (ICT) en apart netwerk (Vlan) aan. Geef de productiemachines alleen toegang tot het internet wanneer dat nodig is.

ONVEILIG: Een firewall in je netwerk is de eerste lijn van verweer tegen aanvallen vanuit het internet op je netwerk. Als er geen firewall aanwezig is of deze wordt niet up-to-date gehouden, is het risico groter dat je slachtoffer wordt van malware of een hack.

Goed dat er van een Next-Gen firewall gebruik wordt gemaakt en deze up-to-date wordt gehouden door jullie IT-leverancier. De machines in de fabriekshal zijn echter aangesloten op hetzelfde netwerk als het kantoor. Wij raden jullie aan om voor de productieomgeving een apart netwerk aan te leggen dat gescheiden is van het kantoornetwerk. Sluit de productiemachines in de fabriekshal af van het internet en geef hen alleen toegang tot het internet wanneer dat nodig is, in jullie geval om updates uit te voeren. Koppel ze daarna weer los van het internet, zodat de machines niet meer van buitenaf bereikbaar zijn.

TECHNIEK

Maak van de productiesystemen, configuraties en de e-mail ook back-ups. Verleng de bewaartijd van de back-ups.

ONVEILIG: Het is belangrijk om back-ups van al je data te maken. Als je geen back-ups hebt kun je flinke schade oplopen bij een incident. Denk bijvoorbeeld aan het verlies van de klantgegevens. Test de back-ups ook regelmatig. Moderne ransomware en virussen openbaren zich pas na een tijd waardoor de bestanden in de back-ups ook versleuteld en besmet zijn.

Het back-upproces van de bestanden en het ERP-systeem lijkt goed op orde met back-ups naar meerdere locaties, echter worden deze al na twee weken overschreven. Van de productiesystemen, de configuraties en de e-mail worden nog geen back-ups gemaakt. Wij raden jullie aan ook van de productiesystemen, de configuraties en de e-mail back-ups te maken. Bewaar de back-ups ook langer, tot minimaal een jaar terug. Een retentietijd van twee weken is doorgaans erg kort. Als ransomware de bestanden versleutelt en jullie komen daar pas na een maand achter, dan zijn de back-ups nutteloos. Gemiddeld komt ransomware pas na drie maanden aan het licht. Bewaar voldoende back-ups om ver genoeg in de tijd terug te gaan, bijvoorbeeld 30 dagen een dagelijkse back-up en bewaar vervolgens 12 maanden een maandelijkse back-up.

TECHNIEK

Zorg dat de API-koppelingen veilig zijn en laat deze testen.

ONVEILIG: De meeste applicaties, met name de eerste versies, bevatten veiligheidslekken. Ook als er ontwikkeld wordt met bestaande tools of low- of no-code ontwikkelomgevingen kunnen simpele beveiligingsinstellingen vergeten worden. Hackers maken graag gebruik van onbeschermde formulieren om spam te versturen of code op het platform uit te voeren, met alle gevolgen van dien.

Jullie ontwikkelen in samenwerking met een derde partij een eigen ERP-systeem. Daar worden code reviews op uitgevoerd. Deze derde partij is ook gecertificeerd. Tussen het ERP-systeem en de productiemachines liggen zogenaamde API-koppelingen. Deze koppelingen zijn niet getest op veiligheid. Wij raden jullie aan deze te laten testen door een onafhankelijke partij. Voer een pentetst en/of security audit op deze koppelingen uit, om te achterhalen waar de eventuele kwetsbaarheden zitten.

MEDEWERKERS

Stel een wachtwoordbeleid op en gebruik een wachtwoordmanager. Vervang de zwakke wachtwoorden op de computers in de fabriekshal.

ONVEILIG: Als je geen wachtwoordbeleid hebt, is de kans groot dat medewerkers voor meerdere accounts dezelfde wachtwoorden en/of zwakke wachtwoorden gebruiken. Als van één account de gegevens lekken, is het voor een crimineel eenvoudig om ook andere accounts binnen te dringen. Als hackers toegang krijgen tot de (bestel)pagina's van leveranciers, dan kunnen ze valse bestellingen plaatsen en deze ergens anders laten afleveren of spam en spookfacturen proberen te versturen.

Jullie huidige wachtwoorden zijn 8 karakters lang en bestaan uit meerdere tekens. De medewerkers dienen deze twee keer per jaar te wijzigen. Op de computers in de fabriekshal staan zwakke wachtwoorden ingesteld. Wij adviseren een sterker wachtwoordbeleid op te stellen en te gaan hanteren en met alle medewerkers afspraken te maken hoe ze met wachtwoorden om moeten gaan. Neem in het beleid op dat iedereen sterke (minimaal 16 karakters), unieke en niet herleidbare wachtzinnen en voor elk account gebruikt. Van de medewerkers is het niet bekend of zij hun wachtwoorden onthouden of opslaan. Wij raden jullie aan om een wachtwoordmanager te gebruiken om alle wachtwoorden veilig in op te slaan. Deze dwingt sterke wachtwoorden af en voorkomt hergebruik van wachtwoorden.

TECHNIEK

Installeer een certificaat op de website en beveilig de beheerpagina.

ONVEILIG: Je websitebezoekers lopen het risico gehackt te worden als je niet de meest actuele internetstandaarden toepast. Als zij bijvoorbeeld via een contactformulier op je website gegevens naar jou verzenden, kunnen criminelen deze gegevens onderscheppen als deze niet (goed) versleuteld zijn.

Wij hebben de website van buitenaf gecheckt op een aantal standaard beveiligingsmaatregelen. Goed dat jullie een certificaat geïnstalleerd hebben, maar we zien hier nog veel verbeteringen mogelijk. De volgende zaken staan niet (goed) ingesteld: DNSSEC, de automatische verwijzing naar de beveiligde (HTTPS) versie, HSTS, het gebruik van een verouderde TLS versie (versie 1.0 of 1.1) en de betrouwbaarheid of de geldigheidsduur van de certificaat (chain), Wij raden aan deze opties te gaan ondersteunen of te verbeteren. Vaak is dit vrij eenvoudig te regelen door de websitebouwer, de hostingspartij en/of de partij die jullie domein(en) beheert. De beheerpagina blijkt ook niet extra beschermd te zijn. De beheerpagina is via het internet toegankelijk. We adviseren hier minimaal een Captcha beveiliging op te zetten om geautomatiseerd inloggen tegen te gaan, maar het liefst zien we hier ook 2FA en/of whitelisting.

WETGEVING

Ga aan de slag met de AVG en leg de benodigde registers aan.

ONVEILIG: Voldoe je niet aan de AVG dan riskeer je hiermee een boete van de Autoriteit Persoonsgegevens (AP). Deze boete kan oplopen tot 4% van je jaaromzet. De AP kan al een onderzoek instellen naar aanleiding van een klacht van slechts 1 klant.

Goed dat jullie i.v.m. de AVG een privacyverklaring aangelegd hebben. Wij hebben deze gecontroleerd en deze voldoet aan de gestelde eisen. Wij raden aan om verder met de AVG aan de slag te gaan. De AVG stelt ook eisen aan hoe jullie om moeten gaan met persoons- en klantgegevens. Inventariseer waar jullie deze gegevens allemaal opslaan en met welke reden en leg dit vast in een verwerkersregister. Jullie dienen een datalekregister aan te leggen waarin jullie bijhouden wat er met betrekking tot de gegevens fout is gegaan.

TECHNIEK

Overweeg het netwerk actief te (laten) monitoren.

ONVOLDOENDE: Als je je netwerk niet monitort, dan heb je geen inzicht in wat er op je netwerk gebeurt. Tegen de tijd dat je ontdekt dat er schadelijke activiteiten plaats vinden is het vaak al te laat.

Jullie IT-leverancier kijkt (met toestemming) op afstand mee op het netwerk. Het netwerk wordt niet actief gemonitord op bijvoorbeeld vreemd gedrag van de computers of op mislukte inlogpogingen van buitenaf. Wij raden jullie aan de mogelijkheden van actieve monitoring met hen te bespreken. Zij kunnen op basis hiervan de beveiliging versterken. In ons securitypakket zit ook een vulnerability scan inbegrepen. Dit geeft goed inzicht in de kwetsbaarheden van jullie website en netwerk en je ontvangt direct een melding als er een kritisch of onveilig probleem ontdekt wordt.

KETENVEILIGHEID

Analyseer de risico's en de impact die leveranciers en afnemers op jouw netwerk en bedrijfsprocessen hebben.

ONVOLDOENDE: Als je vooraf geen afspraken hebt gemaakt kun je nergens op terugvallen. Als je geen goede afspraken hebt gemaakt of niet duidelijk is wat er in de contracten staat, raak je snel in conflict als er een incident of datalek optreedt. De kosten zijn dan vaak voor eigen rekening.

Er is een sterk afhankelijk van andere partijen, zoals leveranciers, aanvullende dienstverleners en afnemers, met name als het gaat om de productieomgeving. Een cyberaanval op een van deze partijen binnen je keten heeft een grote impact op jullie bedrijf. Voer een risicoanalyse uit om inzicht te krijgen in de mogelijke risico's, impact en kosten en tref op basis hiervan extra maatregelen. Controleer de SLA's ook op bereikbaarheid, (uptime)garantie en aansprakelijkheid.

WETGEVING

Check de verwerkersovereenkomsten en de opslag van data binnen Europa.

ONVOLDOENDE: Heb je geen verwerkersovereenkomst met partijen die wel persoonsgegevens (dit begint al met een naam of e-mail) voor je verwerken? In het uiterste geval kan de Autoriteit Persoonsgegevens je een boete opleggen.

Met een aantal partijen zijn verwerkersovereenkomsten afgesloten, maar nog niet allemaal. Wij adviseren na te gaan aan welke partijen jullie gegevens doorgeven en welke partijen gegevens voor jullie verwerken. Denk aan jullie web- en IT-leveranciers, software leveranciers, nieuwsbrieven, etc. Maak inzichtelijk welke verwerkersovereenkomsten jullie hiermee hebben, controleer of ze nog up-to-date zijn en/of sluit deze alsnog af. Controleer ook of jullie data in de cloud (OneDrive) binnen Europa opgeslagen is. Het Hof van Justitie van de Europese Unie (EU) heeft in juli 2020 het EU-VS privacy shield (privacy schild) ongeldig verklaard in de zaak Schrems II. Dat betekent dat organisaties in de EU geen persoonsgegevens aan de Verenigde Staten (VS) meer mogen doorgeven op grond van het privacy shield.

WETGEVING

Zet een privacyverklaring op de website.

KAN BETER: De AVG schrijft voor dat je de bezoekers en klanten informeert over de verwerking van hun persoonsgegevens. Dit doe je bijvoorbeeld in een privacyverklaring. Als je je klanten niet informeert kan de Autoriteit Persoonsgegevens je een boete opleggen. Onveilige formulieren op de website worden misbruikt voor hacks en om spam te versturen. Als er geen beveiligchecks plaatsvinden kan bijvoorbeeld code via het formulier op de website uitgevoerd worden en de achterliggende database gehackt worden. Zonder checks of spamfilter kan het formulier misbruikt worden om spamberichten te versturen. De berichten worden dan vaak onder jouw naam verstuurd naar jouw eigen organisatie of naar buiten toe.

Goed dat jullie wel al een privacyverklaring hebben maar deze staat nog niet op jullie website. Dit is wel verplicht volgens de AVG. Op de website staat een contactformulier waarmee jullie gegevens verwerken. Geef in de privacyverklaring aan welke gegevens jullie precies verwerken en met welk doel. Voeg aan de formulieren een vinkje toe waarin jullie expliciet aan de bezoeker de toestemming vragen voor de verwerking van zijn of haar persoonsgegevens. Zet ook hier een link naar de privacyverklaring.

TECHNIEK

Op alle computers en servers draait een commercieel antiviruspakket.

GOED: Op allerlei manieren kunnen besmette bestanden op je computer terechtkomen (denk aan mails, opslag in de cloud, etc.). Als je dit niet scant is het risico groter dat je besmet raakt met malware. Windows Defender en gratis antivirusprogramma's beschermen vaak goed tegen virussen, maar een commercieel programma biedt bredere bescherming, zoals tegen phishing en crypto- en ransomware.

Op alle servers en computers op het kantoor en in de fabriekshal draait een commercieel antivirusprogramma van BitDefender.

NOODPROCEDURE

Er is een noodprocedure aanwezig.

GOED: Als je geen gedocumenteerde noodprocedure hebt, dan is de kans groot dat medewerkers niet exact weten wat er moet gebeuren in het geval van een cyberincident. In alle hectiek kunnen fouten je dan duur komen te staan. Denk bijvoorbeeld aan het niet (tijdig) melden van een datalek of aan malware dat zich steeds verder verspreid.

Bij een cyberincident weten zowel de kantoormedewerkers als de medewerkers op de werkvloer wat te doen. Jullie wie jullie moeten bereiken, in dit geval de IT-leverancier en de leverancier van de productiesystemen (OT). Er is een bellijst aanwezig met noodnummers en die is onder de medewerkers uitgedeeld.

MEDEWERKERS

Er is scheiding tussen de gegevens aangebracht.

GOED: Niet afgeschermde persoonsgegevens liggen sneller op straat. Een virus of ransomware kan op meerdere plekken schade aanrichten als de toegang tot de gegevens niet beperkt is.

Goed dat jullie scheiding tussen de gegevens hebben aangebracht op zowel map-niveau als binnen de applicaties. Er zijn rechten ingesteld en deze worden actief beheerd door de IT-afdeling.

NOODPROCEDURE

Bij een datalek weten jullie wat er moet gebeuren.

GOED: Een datalek kan al een e-mail met gevoelige informatie naar een verkeerd adres zijn of een laptop of mobiele telefoon die verloren of gestolen is. Het te laat melden van een datalek kan leiden tot een boete van de autoriteit persoonsgegevens.

Er is een functionaris gegevensbescherming aanwezig. Jullie wie jullie moeten bereiken en er is een document met instructies aanwezig voor de medewerkers.

KETENVEILIGHEID

Er is inzicht in de keten(veiligheid).

GOED: Als je geen inzicht hebt in de keten of ketenveiligheid, dan is het vaak onduidelijk waar het probleem zich voordoet en/of wie aansprakelijk is. Onveilige koppelingen met externe systemen vormen vaak een risico dat hackers via die weg je netwerk binnenkomen.

Jullie hebben goed inzicht welke partijen toegang hebben tot jullie gegevens en systemen en welke partijen gegevens voor jullie verwerken. Dit is in kaart gebracht. Ook de API-koppelingen zijn in kaart gebracht.

ADVIES

ALGEMENE ADVIEZEN

ALGEMENE ADVIEZEN

Stop met het gebruik van USB-sticks en overweeg de USB-poorten te blokkeren.

Virussen verspreiden zich vaak via USB-sticks. USB-sticks kunnen al bij de fabrikant besmet zijn met malware. Zelfs als je de USB-stick formatteert voor gebruikt heb je kans op besmetting met malware.

Wij raden het gebruik van USB-sticks sterk af omdat er op deze manier virussen verspreid kunnen worden. Gebruik liever een versleutelde (cloud)dienst om grote (hoeveelheden) bestanden te versturen. Bespreek het dichtzetten van de USB-poorten met jullie IT-leverancier.

ALGEMENE ADVIEZEN

Vergrendel de computers automatisch en/of laat medewerkers hun computer vergrendelen.

Een concurrent of crimineel zit binnen no time in je bedrijfsgegevens of netwerk op het moment dat je een kop koffie gaat halen en je computer onbeheerd achterlaat.

Zorg dat op alle computers een automatische vergrendeling van enkele minuten ingesteld staat. Laat alle medewerkers er ook een gewoonte van maken om handmatig hun computer te vergrendelen als ze even hun werkplek verlaten. Met een simpele short cut: Windows-toets + L (Windows) of Control-Command-Q (Mac) vergrendel je de computer handmatig. Ontvangen jullie bezoekers en bestaat er een kans op meekijken? Er zijn ook privacy schermen verkrijgbaar. Dit is een plastic plaat die je op het scherm zet en de kijkhoek drastisch vermindert, zodat meekijken een stuk moeilijker wordt.

ALGEMEEN

ORGANISATIE

Op 1 juli voerde ik de Cyber Scan uit. De organisatie zag er toen als volgt uit.

- Bij Bouw Groep werken 56 medewerkers, waarvan 18 op het kantoor. Er is een buitendienst en jullie werken ook met oproepkrachten.
- De IT is uitbesteed aan de IT-leverancier ABC-ICT. Met hen is een onderhoudscontract afgesloten. Jullie werken met PC's, laptops, tablets en mobiele telefoons. Jullie werken via een remote desktop verbinding. Op de computers staat Windows 10 geïnstalleerd. De server draait in de cloud. Op de servers zijn netwerkschijven aangesloten voor de opslag van de gegevens. Er wordt ook vanuit huis gewerkt.
- Jullie werken o.a. met Office 365 voor de e-mail, OneDrive, SharePoint, Teams, Numbers, Exact Online en Account View. Er is een eigen ERP (Enterprise Resource Planning) systeem voor het automatiseren en beheren van verschillende processen binnen het bedrijf. Deze is gekoppeld aan de machines in de productiehal. De personeelsadministratie is uitbesteed en jullie werken samen met een arbodienst.
- Jullie verwerken bijzondere gegevens waaronder: BSN, identiteitsscans en Building Information Modellen (BIM). Ook worden er voor bepaalde projecten extra documenten met persoonsgegevens vastgelegd, zoals een Verklaring Omtrent Gedrag (VOG), certificaten, medische keuringen en Opsporen Conventionele Explosieven (OCE). Jullie bewaren ook Cv's.
- De meeste gegevens staan opgeslagen in de applicaties en het ERP-systeem, op de netwerkschijf en in OneDrive.

- Jullie grootste zorgen omtrent de cybersecurity gaan uit naar hacks, ransomware, het niet verder kunnen werken en toegang tot de productiesystemen in de fabriekshal.
- Bouw Groep is gehuisvest in een eigen pand. Het bedrijf heeft meerdere vestigingen. Er worden geen ruimtes of netwerken gedeeld met anderen.