databalance
managed IT solutions

SJ solutions
datamanagement

Cybersecurity

Het reduceren van risico's

Inleidend

De meeste artikelen over cybersecurity beginnen met een verontrustend getal over de hoeveelheid geslaagde cyberaanvallen. Dit is enerzijds terecht, want het aantal cyberaanvallen is ook verontrustend. De voorbeelden zijn wekelijks in het nieuws. Anderzijds is het beveiligen van IT-infrastructuur en werkplekken van alle tijden maar wordt er nu simpelweg meer van ons gevraagd. Cybersecurity is geen optie meer of een 'tick in the box' maar een complexer wordende set van risico's en maatregelen. Maatregelen die bepalend zijn voor de continuïteit en het succes van uw organisatie.

De uitdaging van beveiliging zit in het feit, dat er niet één oplossing, toverformule of maatregel bestaat die alle risico's afdekt. Het is, als gezegd, een complexer wordende set van maatregelen om de risico's te reduceren. Hierin spelen niet alleen techniek en processen een belangrijke rol maar ook de cultuur en de 'soft controls'. De kunst is om tot een set van maatregelen te komen, zowel qua techniek als cultuur, die de kans op een aanval op uw organisatie zo klein mogelijk maakt. In dit artikel zetten we een aantal aandachtspunten en mogelijkheden voor u onder elkaar.

Kort samengevat:

- Het is belangrijk om inzicht te hebben (en te houden) in de kwetsbaarheden in het netwerk. Veel aanvallen maken gebruik van een (bestaande) kwetsbaarheid of misconfiguratie.
- Hoe alert gebruikers ook zijn, het is verstandig om de werkplekken – de zogenaamde endpoints - in de gaten te houden op vreemd gedrag.
- Een hack of ransomware aanval richt zich ook op de back-up, dus dit vraagt meer van de back-up voorziening en de herstelmogelijkheden.
- In veel organisaties is er nog laaghangend fruit, zoals een passwordmanager, waarmee de beveiliging sterk is te verbeteren.
- Een cultuur waarin 'speak up' de norm is, is net zo belangrijk als de (technische) voorzieningen.

Kwetsbaarheden inzichtelijk maken

Veel geslaagde cyberaanvallen maken gebruik van een kwetsbaarheid in software. Welke software ook wordt gebruikt, er komen altijd updates uit en als deze updates niet worden uitgevoerd, dan is dit een 'achterdeur' om binnen te komen. Deze kwetsbaarheden in software, bevinden zich in alle lagen van het netwerk. Op servers, firewalls, werkplekken maar ook op switches, accesspoints etc. Eigenlijk alles met een 'verbinding' is ook een aanvalsoptie. Door de toename van het aantal smart devices (IoT), raken apparaten uit zicht. Om grip te krijgen op kwetsbaarheden is het slim om Vulnerability Management in te zetten. Dit is een oplossing die continu kijkt welke (software) versie actief is op alle componenten in het netwerk en of er kwetsbaarheden zijn in de IT-infrastructuur die gemitigeerd (bijgewerkt) moeten worden. Hierdoor kunnen kwetsbaarheden bijgewerkt worden, voordat ze een probleem worden of worden 'misbruikt' door derden. Er zijn diverse opties en rapportages waarmee Vulnerability Management helemaal op maat en passend kan worden gemaakt voor uw (beheer)organisatie. Hierdoor heeft u grip op- én inzicht in de kwetsbaarheden.

Zo sterk als de zwakste schakel

Alhoewel de security awareness toeneemt en gebruikers best alert zijn, blijven de werkplekken – de endpoints – kwetsbaar en een belangrijke aanvalsoptie. Sommige (phishing) e-mails, websites en meldingen zijn erg lastig van echt te onderscheiden door spoofing en slimme social engineering. Hoe goed gebruikers ook opletten, een fout is snel gemaakt en daarom is het slim om gebruik te maken van Endpoint Protection. Het één sluit het ander niet uit. Ook met Endpoint Protection moeten gebruikers alert zijn en blijven. Met Endpoint Protection wordt er naar 'het gedrag' van de werkplekken gekeken. Dit gaat dus verder dan de traditionele antivirus en het controleren op updates. Endpoint Protection kijkt naar verdachte patronen, zoals het openen en uitvoeren van scripts. Afhankelijk van de activiteiten die

worden waargenomen en het bijbehorende risico, kunnen werkplekken ook direct en automatisch geïsoleerd worden. Ook hier geldt, dat er niet één optie of mogelijkheid is voor de endpoints. Er zijn diverse opties en voorzieningen, die uw gebruikers aanvullend ondersteunen en beschermen.

En als het dan toch misgaat

Het is misschien geen prettige gedachte maar u zult ook moeten nadenken over voorzieningen en maatregelen, wanneer u onverhoopt wel wordt geraakt door een aanval of hack. In dit geval moet u terug kunnen vallen op een back-up voorziening. En wat geldt voor endpoints en het netwerk, geldt ook voor back-ups: de traditionele kopie en tape volstaat niet meer in een tijd waar hackers het gehele netwerk gijzelen. Vaak zit (staat) de hack ook al op de back-up die u heeft gemaakt en wordt er (nog) geen gebruik gemaakt van 'immutability'.

Het goede nieuws is, dat datamanagement ook in ontwikkeling is. Zo wordt er gebruik gemaakt van 'write once, read many' (WORM) storage oplossingen en zijn er diverse mogelijkheden om de back-ups versleuteld extern op te slaan én met behulp van een separate disaster recovery omgeving te herstellen. Dit is een omgeving, geïsoleerd van productie, om de hack te analyseren, te mitigeren en te herstellen. Dit betekent dat u, mocht u onverhoopt toch worden gehackt, het herstel inclusief geautomatiseerde testruns is geborgd en u de (reputatie)schade en het dataverlies kunt beperken.

Laaghangend fruit

Naast de genoemde oplossingen en mogelijkheden, zien we ook nog met regelmaat, dat lang niet iedere organisatie gebruik maakt van (gangbare) oplossingen zoals een passwordmanager. Dit zijn eenvoudige en relatief goedkope oplossingen, die de beveiliging significant verbeteren. Dit laaghangend fruit is belangrijk om mee te nemen en een goede manier om de risico's op korte termijn (sterk) te reduceren.

Ook cultuur is bepalend

Naast technische maatregelen en processen zijn ook de cultuur en de soft controls heel belangrijk voor de (informatie)beveiliging van een organisatie. Beveiliging is door de toenemende complexiteit geen jaarlijkse 'tick in the box' tijdens het certificeringstraject maar doorlopend in ontwikkeling en onderdeel van de bedrijfsfilosofie. Zo dient iedere medewerkers, ongeacht rol, verantwoordelijkheid of ervaring, de vrijheid te voelen zich uit te spreken. Een 'speak up' cultuur, zorgt dat risico's vroegtijdig worden gesignaleerd en kunnen worden verholpen. Het zorgt voor een hogere standaard, minder aannames en meer kwaliteit. Beveiliging is niet uitsluitend de verantwoordelijkheid van een individu of afdeling. Alle lagen van de organisatie moeten doordrongen zijn van het belang van zorgvuldig omgaan met data en de risico's.

Lang verhaal kort

Om de continuïteit van uw organisatie te borgen, kunt u een aantal technische maatregelen nemen die de kans op een hack of aanval sterk reduceren. Denk aan het beschermen van werkplekken en het inzichtelijk maken van kwetsbaarheden. Maar ook aan de voorzieningen indien u wel wordt getroffen. Naast deze technische maatregelen zullen de cultuur en de soft controls, waarin iedereen zich durft uit te spreken, het verschil maken.

Laten we eens sparren

Wij hanteren het uitgangspunt dat 'niemand de wijsheid in pacht heeft'. Dit betekent dat wij open het gesprek aangaan en transparant onze kennis delen. Hierin horen we ook graag uw bevindingen en ervaringen.

Door in alle openheid alle opties te bespreken, komen we gezamenlijk verder. Daarbij is iedere organisatie verschillend qua business context en business requirements. Kortom, laten we eens sparren, we gaan graag het gesprek aan!

Neem contact op met één van onze specialisten:

- Martin Koster (Solutions Architect) – martin.koster@databalance.eu
- Ben Velders (Solutions Architect) – b.velders@sj-solutions.nl
- Sebastiaan Bakker (Security Officer) – s.bakker@sj-solutions.nl
- Nordi Malih (CEO) – nordi@databalance.eu