Technische QuickScan

Technische Cybersecurity		
1 Back up & Restore		
	Vraag	Risico
1-1	Van welke systemen worden back-ups gemaakt? Antwoord: DATA, virtuele servers	Indien geen back-ups gemaakt worden kan gegevensverlies optreden bij incidenten of hardware failure
1-2	Wat voor soort back-ups zijn dit? (Full, incremental, snapshots) Antwoord: combinatie van de bovenstaande	Incremental back-ups en snapshots kunnen een systeem niet volledig herstellen
1-3	Wat is de frequentie van deze back-ups? Antwoord: dagelijks voor data, dagelijks voor Active directory, maandelijks voor vm's	Weinig back-ups zorgen mogelijk voor groter verlies van data
1-4	Welke systemen worden NIET geback-upt? Antwoord: /	Deze systemen kunnen volledig verloren gaan
1-5	Waarom niet? Antwoord:	-
1-6	Worden er volledige restore tests uitgevoerd van alle geback-upte systemen? Antwoord: nee	Het is mogelijk dat er fouten zitten in het restore proces of in de gebruikte programmatuur

1-7	Wat is de frequentie van deze restore tests? Antwoord:	
2	**Security Testing**	
	Vraag	Risico
2-1	Worden er periodieke penetratietesten uitgevoerd? Antwoord: JA	Bedrijf heeft geen inzicht in kwetsbaarhe- den van applicaties en systemen
2-2	Welke systemen worden er getest? Antwoord: servers	Bedrijf heeft geen inzicht in kwetsbaarhe- den van applicaties en systemen
2-3	Wordt dit gedaan door wisselende partijen? Antwoord: nee, intern	Verschillende partijen gebruiken verschil- lende benaderingen met als gevolg moge- lijk groter inzicht in de veiligheid van de applicatie
2-4	Worden her testen uitgevoerd van eerdere penetra- tiestesten? Antwoord: nvt.	Hierdoor wordt opvolging van bevindingen gecontroleerd
2-5	Worden bevindingen altijd opgevolgd? Antwoord: NEE	Onvoldoende opvolging kan leiden tot blij- vende en/of ondergeschoven kwetsbaar- heden

3	**Secure Coding**	
	Vraag	Risico
3-1	Worden er risicoanalyses uitgevoerd bij het opstarten van een project? Antwoord: NVT	Het is onduidelijk welke risico's gelopen worden tijdens en bij go-live van het pro- ject
3-2	Welke personen zijn hierbij betrokken / verantwoorde- lijk? Antwoord: NVT	Er dienen security experts bij betrokken te zijn
3-3	Wordt er gebruik gemaakt van secure coding guideli- nes? (OWASP) Antwoord: NVT	De applicatie loopt groter risico op kwetsbaarheden met hogere herstelkos- ten
3-4	Wordt er gebruik gemaakt van andere best practi- ces/guidlines? (ASVS) Antwoord: NVT	De applicatie loopt groter risico op kwetsbaarheden met hogere herstelkos- ten
4	**Scheiding van systemen**	
	Vraag	Risico
4-1	Zijn alle systemen, applicaties, DB's, interfaces, etc. duidelijk in kaart? Antwoord: NVT	Onvoldoende zicht op applicatieland- schap kan leiden tot outdated systemen

4-2	Is er een duidelijke scheiding tussen OTAP? (fysiek/lo- gisch) Antwoord: NVT	In geval van calamiteiten worden niet alle omgevingen aangetast.
4-3	Is functiescheiding hierop van toepassing? Antwoord: NVT	Er kunnen ongecontroleerde wijzigingen worden doorgevoerd
4-4	Wordt er bij architectuur rekening gehouden met schei- ding van systemen? (Webserver, applicatieserver, DB- server, etc.) Antwoord: NVT	Zonder scheiding is het aanvalsoppervlak groter en mogelijke impact van inbraak groter
4-5	Word er gebruik gemaakt van een DMZ? Antwoord: NVT	Zonder scheiding is het aanvalsoppervlak groter en mogelijke impact van inbraak groter
4-6	Word er gebruik gemaakt van Reverse proxy's? Antwoord:	
5	**Logging**	
	Vraag	Risico
5-1	Op welke systemen wordt logging toegepast? Antwoord:	In geval van incidenten kan niet worden teruggegrepen op logging

5-2	hoe uitgebreid is deze logging? Antwoord:	In geval van incidenten kan te weinig (nuttige) informatie worden gevonden
5-3	Wie heeft toegang tot de logging? Antwoord:	Ongeautoriseerde toegang kan leiden tot wijzigen/verwijderen van logging
5-4	Wordt de logging actief gemonitord? Antwoord:	Onregelmatigheden worden niet op tijd opgemerkt
5-5	Wordt de logging periodiek gecheckt op onregelmatig- heden? Antwoord:	Onregelmatigheden worden niet op tijd opgemerkt
6	**Security incidenten**	
	Vraag	Risico
6-1	Is er een centraal aanspreekpunt voor het melden van security incidenten? Antwoord:	Security incidenten worden niet gemeld
6-2	Hoe is de opvolging hiervan geregeld? Antwoord:	Security incidenten blijven bestaan, mo- tivatie tot melden verdwijnt
6-3	Hebben klanten en/of buitenstaanders de mogelijkheid security kwetsbaarheden te melden?	Kwetsbaarheden worden op andere on- controleerbare manieren bekend

	Antwoord:	
6-4	Zo ja, hoe vind de opvolging hiervan plaats? Antwoord:	Security incidenten blijven bestaan, mo- tivatie tot melden verdwijnt
6-5	Zo nee, hoe wordt omgegaan wanneer dit wel gebeurt? Antwoord:	Security incidenten blijven bestaan, mo- tivatie tot melden verdwijnt
7	**Authenticatie**	
	Vraag	Risico
7-1	Worden sterke wachtwoorden voor alle applicaties en systemen afgedwongen? Antwoord:	Zwakke wachtwoorden zijn gemakkelij- ker te kraken
7-2	Wordt gebruik gemaakt van 2factor authenticatie voor gevoelige of kritieke systemen? Antwoord:	Wachtwoorden zijn mogelijk eenvouding af te kijken, raden of kraken
7-3	Zijn interne systemen afgeschermd van buiten? Antwoord:	Aanvalsoppervlak van organisatie is groot
7-4	Wordt ip restrictie toegepast? Antwoord:	Aanvalsoppervlak van organisatie is groot
7-5	Wordt er gebruik gemaakt van VPN?	VPN kan een veilige manier van werken

	Antwoord:	op afstand zijn
7-6	Hoe is de toegang hiertoe geregeld? Antwoord:	In geval van compromittering leidt ruime toegang tot grotere impact
7-7	Welke applicaties/servers/etc. zijn er te benaderen via de VPN? Antwoord:	Aanvalsoppervlak van organisatie is groot
7-8	Wordt er gebruik gemaakt van 2fa voor de VPN? Antwoord:	Wachtwoorden zijn mogelijk eenvoudig af te kijken, raden of kraken
8	**Communicatie**	
	Vraag	Risico
8-1	Wordt er voor alle systemen gebruik gemaakt van HTTPS? Antwoord:	Onversleutelde verbinding is mogelijk uit te lezen; identiteit van website kan niet geverifieerd worden
9	**Opslag**	
	Vraag	Risico
9-1	Zijn systemen versleuteld? (BitLocker) Antwoord:	Onversleutelde systemen kunnen een- vouding worden uitgelezen

9-2	Is het toegestaan gevoelige data op te slaan op lokale harde schijf? Antwoord:	Lokaal opgeslagen data is eenvoudig uit te lezen (oplossing: BitLocker)
9-3	Wordt er gebruik gemaakt van onversleutelde USB- sticks? Antwoord:	Oversleutelde USB sticks met gevoelige informatie zijn zeer eenvoudig uit te le- zen en er is grote kans op verlies of dief- stal
9-4	Wordt er gebruik gemaakt van cloud-opslag? Antwoord:	Cloud opslag kan onderhevig zijn aan an- dere wetgeving en mogelijke verlies van data betekenen bij calamiteiten leve- rende partij
9-5	Wordt hiervoor gebruik gemaakt van 2fa? Antwoord:	Wachtwoorden zijn mogelijk eenvouding af te kijken, raden of kraken
9-6	Wordt opslag die kapot is of aan het einde van de levensduur door een specialistisch bedrijf verwijderd? Antwoord:	Onversleutelde systemen kunnen een- voudig worden uitgelezen
10 Toegang		
	Vraag	Risico
10-1	Is toegang tot server ruimtes beperkt?	ongeautoriseerde toegang tot of wijzigingen van systemen

	Antwoord:	
10-2	Zijn USB poorten afgeschermd? Antwoord:	Besmette USB sticks kunnen systemen infecteren en gegevens stelen
10-3	Is het mogelijk gebruik te maken van UTP kabels om op het netwerk te komen met willekeurige apparaten? Antwoord:	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-4	Wordt er gebruik gemaakt van MAC whitelisting? Antwoord:	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-5	Is er beveiligde Wifi aanwezig? Antwoord:	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-6	Is er een scheiding tussen interne en gasten wifi? Antwoord:	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-7	Is er filtering actief op het netwerk (ports, websites) Antwoord:	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-8	Wordt er gebruik gemaakt van IPS/IDS Antwoord:	geen monitoring op mogelijke aanvallen
10-9	Zo ja, vind hier actieve monitoring op plaats? Antwoord:	te late reactie op mogelijke aanvallen

11 Updates & Patches		
	Vraag	Risico
11-1	Is er patch management actief? Antwoord:	Geen actuele versies met mogelijk bekende kwetsbaarheden
11-2	Worden applicaties en systemen altijd voorzien van de laatste security updates? Antwoord:	Geen actuele versies met mogelijk bekende kwetsbaarheden
11-3	Blijven applicatiebeheerders op de hoogte van 0-day kwetsbaarheden of andere bekende kwetsbaarheden? Antwoord:	Mogelijk onveilige systemen
11-4	Worden er maatregelen genomen wanneer kwetsbaarheden van toepassing zijn? Antwoord:	Mogelijk onveilige systemen