CNAM ÎLE-DE-France
SEC101

Devoir: Analyse de risques 2

Vous devez faire l’atelier 3 sur l’entreprise DataSecureTech

Atelier 3:

- Partie prenantes
- Évaluation des parties prenantes
- Scénarios stratégiques
    - Chemins d’attaque

Parties Prenantes

PARTIE PRENANTE: Élément (personne, système d’information, organisation, ou source de risque) en interaction directe ou indirecte avec l’objet de l’étude. On entend par interaction toute relation intervenant dans le fonctionnement normal de l’objet de l’étude. Une partie prenante peut être interne ou externe à l’organisation à laquelle appartient l’objet de l’étude.

En interne nous pouvons citer les employés, notamment le personnel de développement, du marketing, la vente, le support client, et de la gestion administrative. Leurs rôles et le développement des produits, la gestion des opérations et interaction avec les clients notamment.

En externe maintenant:

- Les clients, essentiellement les entreprises utilisant les applications de DataSecureTech pour sécuriser leurs propres données. Elles sont les utilisateurs finaux des solutions de l'entreprise. C’est la source principale de revenus, et le retour d'expérience est crucial pour l'amélioration des services.

- Les partenaires pouvant être des entreprises technologiques, fournisseurs de services cloud, et agences de marketing. Collaboration pour le développement des produits, la distribution et le marketing. Essentiel pour l'expansion du marché et la diversification des offres.

- Les fournisseurs par exemple les FAI, de matériel informatique, de logiciels… Ils permettent la fourniture des ressources nécessaires pour les opérations quotidiennes, leurs rôle est critique pour le maintien des infrastructures et la continuité des services.

- Éventuellement des investisseurs, par exemple des institutions finançant la start-up. Ils permettront la fourniture de capitaux pour le développement et/ou la croissance, utile pour les opérations et l'expansion.

- Les autorités régulatrices qui sont les organismes de conformité qui régulent la protection des données personnelles, et de surveillance des pratiques de sécurité et de conformité.Très critique pour assurer la conformité et éviter les sanctions.

Évaluation des Parties Prenantes

PARTIE PRENANTE	CHEMINS D'ATTAQUE STRATÉGIQUES	MESURES DE SÉCURITÉ	MENACE INITIALE	MENACE RÉSIDUELLE
Employés	Accès non autorisé aux informations sensibles; phishing	- Politiques de contrôle d'accès strictes - Formation régulière en sécurité - Authentification multifactorielle	Compromission des informations internes	Risque de phishing réussi malgré la formation
Clients	Vol de données clients; attaque par déni de service (DDoS)	- Chiffrement des données clients - Solutions anti-DdoS - Surveillance continue des systèmes	Perte de données clients et indisponibilité des services	Accès illégal via des comptes compromis
Partenaires	Fuite d'informations confidentielles; attaques indirectes via des partenaires	- Contrats de confidentialité - Évaluation régulière de la sécurité des partenaires - Réseau segmenté et sécurisé	Compromission par un partenaire non sécurisé	Accès non autorisé malgré les contrôles de partenaire
Fournisseurs	Interruption de service par des vulnérabilités des fournisseurs	- Surveillance et audit des fournisseurs - Redondance des services critiques	Dépendance excessive sur un fournisseur	Risque de faille de sécurité chez le fournisseur
Investisseurs	Divulgation non autorisée d'informations financières et stratégiques	- Contrats de non-divulgation - Chiffrement des communications - Contrôles d'accès basés sur les rôles	Fuite d'informations stratégiques	Risque de compromission des informations malgré les contrôles
Autorités Régulatrices	Non-conformité avec les régulations; amendes et/ou sanctions	- Suivi des régulations en temps réel - Mise à jour continue des pratiques de conformité - Rapports de conformité réguliers	Sanctions légales et perte de réputation	Risque de non-conformité résiduelle due à une mise à jour réglementaire

Scénarios Stratégiques

SCÉNARIO STRATÉGIQUE: Chemins d’attaque allant d’une source de risque à un objectif visé en passant par l’écosystème et les valeurs métier de l’objet étudié. Les scénarios stratégiques sont évalués en termes de gravité.

1/ Scénario de violation de données avec un malware
- Source de risque: acteurs malveillants développant un malware sophistiqué, de type APT.
- Chemin d'attaque:
  - Infiltration par e-mail phishing: les cybercriminels envoient des e-mails de phishing à des employés de DataSecureTech contenant des liens ou des pièces jointes malveillantes.
  - Déploiement de malware: lorsqu'un employé clique sur le lien ou ouvre la pièce jointe, le malware est déployé sur le système informatique de l'entreprise.
  - Propagation du malware: le malware se propage à travers le réseau interne, atteignant les serveurs de données sensibles.
  - Exfiltration de données: le malware collecte et envoie des données sensibles (par exemple des données client) vers un serveur de commande et de contrôle externe contrôlé par les attaquants.
- Impact sur l’entreprise:
  - Perte de données sensibles: exfiltration de données sensibles client, entraînant des violations de la confidentialité et des obligations réglementaires.
  - Atteinte à la réputation: perte de confiance des clients et partenaires commerciaux, impactant la réputation de DataSecureTech.
  - Pertes financières: coûts liés à la gestion de la violation, aux amendes réglementaires et à la perte de clients.

2/ Scénario de compromission de l'infrastructure cloud
- Source de risque: exploitation de vulnérabilités dans les services cloud.
- Chemin d'attaque:
  - Exploration de vulnérabilités: les attaquants identifient des vulnérabilités dans les configurations des services cloud utilisés par DataSecureTech.
  - Accès non autorisé: exploitation des vulnérabilités pour obtenir un accès non autorisé aux ressources cloud.
  - Déploiement de logiciels malveillants: les attaquants déploient des logiciels malveillants ou exécutent des scripts pour exfiltrer des données stockées sur le cloud.
  - Interruption de service: les attaquants déclenchent une attaque de déni de service (DdoS) pour perturber les services cloud, rendant les données et services indisponibles.
- Impact sur l’entreprise:
  - Compromission des données client: perte ou exposition des données clients, mettant en danger la confidentialité et la sécurité.
  - Interruptions des services: perturbations des services essentiels, impactant les opérations commerciales et la satisfaction des clients.
  - Pertes économiques: réduction des revenus et coûts élevés pour rétablir la sécurité et la continuité des services.

3/ Scénario de manipulation des données par un employé malveillant
- Source de risque: employé interne mécontent ou corrompu.
- Chemin d'attaque:
  - Accès légitime aux données: un employé dispose de privilèges d'accès légitimes aux systèmes de données sensibles.
  - Modification malveillante des données: l'employé utilise son accès pour modifier des données critiques ou introduire des données incorrectes dans les systèmes.
  - Exfiltration de données: l'employé exporte des données sensibles à des tiers ou à des concurrents.

  - Falsification d’informations: l'employé falsifie des informations pour nuire à l'intégrité des processus métiers ou des décisions stratégiques.
- Impact sur l’entreprise:
  - Atteinte à l'intégrité des données: perte de confiance dans les systèmes de données en raison de la corruption des données.
  - Dommages réputationnels: réputation endommagée en raison de la divulgation ou de la manipulation malveillante des données.
  - Conséquences juridiques: enquêtes et poursuites judiciaires pour non-respect des réglementations sur la protection des données.

4/ Scénario d'exploitation d'une vulnérabilité zero-day
- Source de risque: utilisation de vulnérabilités non corrigées ou inconnues (zero-day).
- Chemin d'attaque:
  - Découverte de la vulnérabilité: les attaquants découvrent une vulnérabilité zero-day dans les systèmes ou applications de DataSecureTech.
  - Exploitation de la vulnérabilité: utilisation de la vulnérabilité pour accéder aux systèmes internes ou déployer des logiciels malveillants.
  - Escalade de privilèges: les attaquants exploitent la vulnérabilité pour escalader leurs privilèges et obtenir un accès administratif.
  - Contrôle du système: les attaquants prennent le contrôle des systèmes critiques ou des réseaux, permettant des actions malveillantes à grande échelle.
- Impact sur l’entreprise:
  - Compromission des systèmes: pertes de contrôle sur les systèmes critiques, entraînant des risques opérationnels majeurs.
  - Perte de confiance: perte de confiance des clients et partenaires en raison de la compromission de la sécurité.
  - Impacts financier: coûts de remédiation élevés pour corriger les vulnérabilités et restaurer les systèmes.

5/ Scénario d'attaque par ransomware
- Source de risque: attaque par rançongiciel.
- Chemin d'attaque:
  - Phishing ou ingénierie sociale: les attaquants utilisent des techniques de phishing ou d'ingénierie sociale pour obtenir des accès initiaux.
  - Déploiement de ransomware: une fois l'accès obtenu, les attaquants déploient le rançongiciel sur les systèmes de l'entreprise.
  - Chiffrement des données: le rançongiciel chiffre les données critiques, rendant les systèmes et les informations inaccessibles.
  - Demande de rançon: les attaquants exigent une rançon pour fournir une clé de déchiffrement.
- Impact sur l’entreprise:
  - Indisponibilité des systèmes: systèmes et données critiques inaccessibles, interrompant les opérations commerciales.
  - Pertes Financières: coût de la rançon et dépenses pour la récupération des données et la remise en état des systèmes.
  - Atteinte à la confiance: perte de confiance des clients et partenaires en raison de l'incapacité à protéger les données.

Chemins d’Attaque

CHEMIN D’ATTAQUE: Suite d’événements distincts que la source de risque devra probablement générer pour atteindre son objectif. Cette terminologie concerne les scénarios stratégiques.

1. Chemin d’attaque: violation de données via un malware

- Source de risque: acteurs malveillants développant un malware.
- Objectif: exfiltration de données sensibles.
- Chemin d'attaque:
    1. Recherche et phishing (préparation): les attaquants collectent des informations sur les employés de DataSecureTech pour cibler des individus susceptibles de tomber dans le piège.
    2. Envoi d’e-mails de phishing (infiltration): des e-mails contenant des liens ou pièces jointes malveillantes sont envoyés aux cibles.
    3. Clic et infection (compromission initiale): un employé clique sur le lien ou ouvre la pièce jointe, activant le malware.
    4. Propagation du malware (établissement): le malware s'étend sur le réseau de l’entreprise, atteignant plusieurs machines.
    5. Accès aux données sensibles (escalade): le malware recherche et accède aux fichiers contenant des informations sensibles.
    6. Exfiltration des données (exfiltration): les données sont transférées vers un serveur externe contrôlé par les attaquants.

2. Chemin d’attaque: compromission de l'infrastructure cloud

- Source de risque: exploitation de vulnérabilités dans les services cloud.
- Objectif: accès non autorisé et perturbation des services.
- Chemin d'attaque:
    1. Identification de vulnérabilités (reconnaissance): les attaquants analysent les services cloud utilisés par DataSecureTech pour identifier des failles.
    2. Exploitation des failles (accès initial): utilisation des vulnérabilités découvertes pour obtenir un accès initial non autorisé.
    3. Accès aux ressources cloud (propagation): les attaquants accèdent à des ressources supplémentaires sur le cloud, élargissant leur contrôle.
    4. Déploiement de malwares ou scripts malveillants (établissement): déploiement de malwares pour exfiltrer des données ou scripts pour perturber les services.
    5. Perturbation des services: les attaquants lancent des attaques DDoS ou perturbent les services cloud, rendant les données et services indisponibles.
    6. Extraction de données (exfiltration): exfiltration des données cloud vers des serveurs externes.

3. Chemin d’attaque: manipulation des données par un employé malveillant

- Source de risque: employé mécontent ou corrompu.
- Objectif: falsification ou exfiltration de données.
- Chemin d'attaque:

1. Accès légitime aux systèmes (préparation): l'employé dispose d’un accès légitime aux systèmes de l'entreprise.
2. Identification des données cibles (reconnaissance): l'employé localise les données sensibles ou critiques qu'il souhaite manipuler ou voler.
3. Modification des données (compromission): l'employé modifie ou falsifie les données pour atteindre ses objectifs malveillants.
4. Exportation des données (exfiltration): l'employé extrait les données sensibles et les transfère à des tiers.
5. Suppression des traces (évasion): l'employé efface les logs ou crée de fausses pistes pour masquer ses actions.
6. Dénonciation ou utilisation des données (utilisation): les données volées sont utilisées pour nuire à l’entreprise ou divulguées publiquement.

4. Chemin d’attaque: exploitation d'une vulnérabilité zero-day

- Source de risque: utilisation de vulnérabilités zero-day.
- Objectif: prise de contrôle des systèmes critiques.
- Chemin d'attaque:
    1. Découverte de la vulnérabilité (reconnaissance): les attaquants identifient une vulnérabilité non corrigée dans les systèmes de DataSecureTech.
    2. Développement d’un exploit (préparation): création d'un exploit pour tirer parti de la vulnérabilité zero-day.
    3. Lancement de l'exploit (accès initial): déploiement de l'exploit pour accéder au système cible.
    4. Escalade de privilèges (établissement): les attaquants escaladent leurs privilèges pour obtenir un accès administrateur.
    5. Installation de backdoors (maintien de l’accès): installation de backdoors pour maintenir un accès à long terme.
    6. Exécution d'actions malveillantes (utilisation): prise de contrôle des systèmes critiques, perturbation des services, ou extraction de données sensibles.

5. Chemin d’attaque: attaque par ransomware

- Source de risque: attaque par rançongiciel.
- Objectif: chiffrement des données pour demande de rançon.
- Chemin d'attaque:
    1. Ciblage via phishing (préparation): envoi d’e-mails de phishing pour obtenir un accès initial aux systèmes.
    2. Installation de rançongiciel (accès initial): une fois l'accès obtenu, le rançongiciel est installé sur les systèmes.
    3. Chiffrement des données (établissement): les données critiques sont chiffrées, rendant les systèmes inaccessibles.
    4. Affichage de la demande de rançon (notification): les attaquants informent l’entreprise de la demande de rançon pour déchiffrer les données.
    5. Perturbation des services: les systèmes restent indisponibles, perturbant les opérations jusqu'à ce que la rançon soit payée ou que les données soient récupérées autrement.

6. Récupération des données (utilisation): en cas de paiement, les attaquants fournissent une clé de déchiffrement, ou les données peuvent être récupérées via des sauvegardes.