CPI congrès des professionnel·le·s de l'information

organisé par la Fédération des milieux documentaires (FMD)

VERS UNE OPTIMISATION DES RESSOURCES ET DES SERVICES

Cyberattaque en bibliothèque: pas de panique!

Une expérience de la Bibliothèque publique de Westmount

Baiocco, Lora, Bibliothécaire, services en ligne et archives
Bouchard, Julie, Bibliothécaire des systèmes et des services techniques

Bibliothèque publique de Westmount

Selon la société de cybersécurité Check Point,

« 2022 [...] a connu un niveau record de cyberattaques en réponse à la guerre russo-ukrainienne. L'éducation et la recherche restent les secteurs les plus visés [...] Dans l'ensemble, les cyberattaques mondiales ont augmenté de 38 % en 2022 par rapport à 2021 ».

Checkpoint Security firm
https://pages.checkpoint.com/cyber-security-report-2023.html

Toronto Public Library Website Update

Sunday, November 5, 5:00 pm: We are actively addressing a cyber security incident that came to our attention on Saturday, October 28.

As a result of the incident, the following services are unavailable: tpl.ca, “your account”, tpl:map passes and digital collections. Public computers and printing services at our branches are also unavailable.

Library branches are open as scheduled. Wifi is available in library branches, and branch telephone lines are working. Materials can be borrowed and returned in branches until further notice.

There continues to be no evidence at this time that the personal information of our staff or customers has been compromised.

TPL has proactively prepared for cybersecurity issues and promptly initiated measures to mitigate potential impacts. We have engaged with third-party cybersecurity experts and law enforcement to help us in resolving this situation.

Based on our progress to date, we anticipate that it will take a week or more before all systems are fully restored to normal operations. However, we expect that some services will be brought back online before then.

Sondage

3 phases d’impact

Cyberattaque / Systèmes non disponibles

Récupération / Atténuation

Adaptation / Ajustements continus

Phase 1: Cyberattaque, Systèmes non disponibles 10 jours

Date: 20 nov. 2022

Impacts sur les services & outils de travail

Non disponible:

- V-Smart (SIGB)
- Site Web de la Bibliothèque/CMS
- Téléphones
- Courriels
- Disques réseau de la Ville

Disponible:

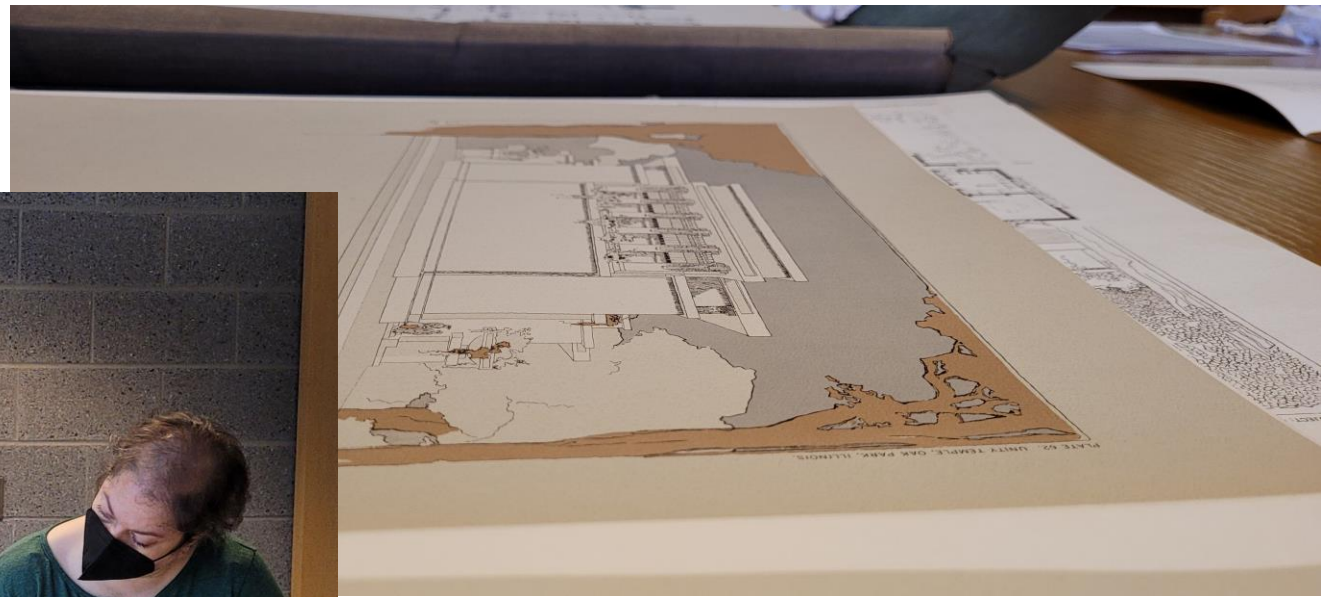
- Internet & Wifi public
- Word, Excel, etc.
- Fichiers locaux (ex. Sauvegardés sur les postes de travail ou dans le cloud)
- Site Web de la Ville
- Certaines bases de données
- Médias sociaux
- Infolettre (Mailchimp)

Services encore accessibles

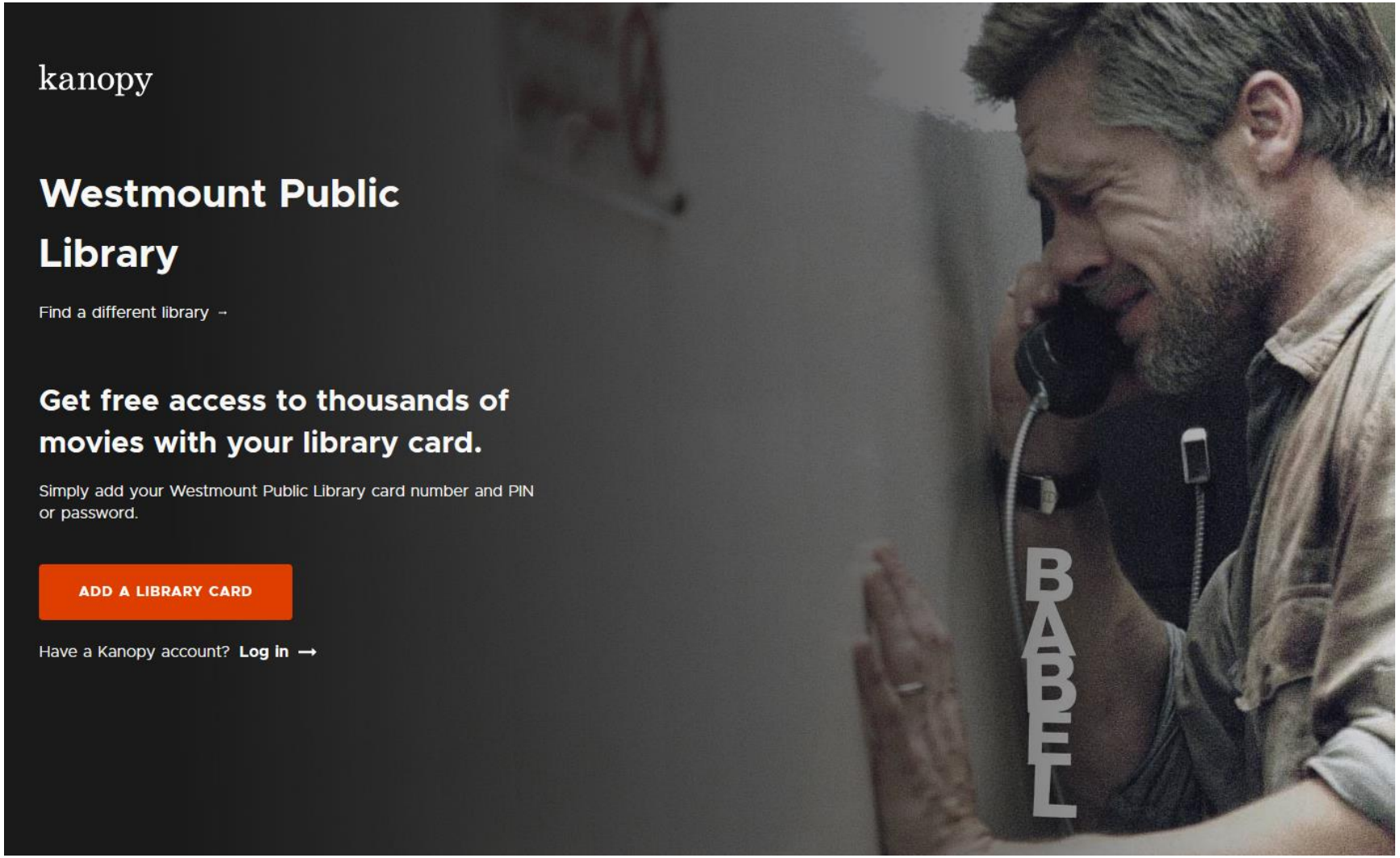
- Espace physique
- Prêts manuels
- Retours (mis de côté)

Tâches qu’il est possible d’accomplir…

- Lecture de rayons
- Préparation matérielle (sauf attribution de cotes)
- Rangement/organisation dans l’espace de travail
- Services tiers pour communications (Facebook, Instagram, Infolettre)
- Rédaction et traduction de communications envers nos abonnés
- Projet spécial de catalogage



SIP2 et Services numériques



📌 Veuillez noter que les services en ligne ne sont pas disponibles en ce moment. Une mise à jour sera communiquée lorsque les services seront rétablis.

❌ Les services suivants sont affectés : site Web, comptes d'abonnés, système de réservation, et services en ligne.

Merci de votre compréhension.

Rançongiciels

La Ville de Westmount piratée

HUGO JONCAS
ÉQUIPE D'ENQUÊTE, LA PRESSE

Lundi en début de soirée, la Ville a publié un communiqué précisant que le piratage a touché « plusieurs serveurs » et causé une « panne informatique ». Le site web de Westmount n'est toutefois pas affecté.

Le gang Lockbit dit avoir 14 téraoctets de données de la Ville en sa possession, soit 14 milliards de kilo-octets, une quantité considérable d'information, plus importante que les autres fuites ayant frappé des organisations québécoises ces derniers mois.

Les pirates au rançongiciel ont fait l'annonce de l'attaque sur leur blogue dimanche, selon ce qu'a pu constater *La Presse* sur le web caché (*dark web*). Ils ont d'abord déclaré qu'ils donneraient seulement deux jours à la municipalité pour payer, mais le gang a ensuite modifié sa page et l'ultimatum s'est allongé à 14 jours.

WESTMOUNT INDEPENDENT

Weekly. Vol. 16 No. 12a | We are Westmount | November 29, 2022

Public Security, winter sports sign-up spared, library hard hit

City internet shut down by cyberattack

By Laureen Sweeney

By press time Friday, November 25 about half the city's email had been restored after cyberattack "pirates" hacked into it over the November 19-20 weekend. The update came from Mayor Christina Smith, who also confirmed that not all the servers had been hacked but would not disclose whether a ransom had been sought.

The cyberattack shut down city email access through westmount.org and also affected some telephone lines linked to them. By Friday however, it was reported that things appeared to be "slowly coming back." The city website continued to operate.

The identity of the hackers, if known, has not yet been revealed "due to the criminal extent of damage."

The city's Public Security Unit was not affected in its phone requests for emergency response, according to its assistant director Kimberley Colquhoun.

The library, however, was reportedly one of the hardest hit, leaving people without the ability to obtain material online and has been asking that borrowed material not be immediately returned until further notice. Staff was on duty and people were able to use many services.

A message on the city's website announced that the city's IT department was working with hired specialists in cyber security "to determine the extent of the attack and restore systems as quickly as possible." It did, however, leave many computers locked down and employees unable to access previous work.

While the city's website was still operating, some recent information expected to have been posted on it appeared not to have been. This included the recording of the YouTube proceedings of the council meeting, but whose webinar functioned as usual Monday, November 21.

"Fortunately," the winter online registration for Sports and Recreation, which opened November 22, was unaffected since it is managed through the outside firm of PD Solutions, said department director Dave Lapointe.

Not everything affected

As well, he said, while he was able to use his computer, he could not access stored information. "Usually when the pirates attack, they get everything, but in our case, they didn't get everything. Some servers were unaffected."

The cyberattack resulted in a notice from the Finance department saying that because it is unable to process bills at this time "we ask for your patience." Once systems have been secured, payments would be processed "quickly."

Mayor Christina Smith who was out of town at the time, added this message to the one on the city's website saying: "I want to tell all Westmounters that our teams are working seriously and diligently to remedy this situation and we will keep you informed."

As a result, the council meeting, November 21, was chaired by Councillor Conrad Peart as pro-mayor and conducted from paper agendas. It was somewhat reminiscent of a dimly lit emergency council meeting carried on during the ice storm of 1998, when typewriters were used.

We welcome your letters

We welcome your letters but reserve the right to choose and edit them. Please limit to 300 words and submit before Friday 10 am to be considered for publication the following week. email us at: editor@westmountindependent.com

MONTREAL GAZETTE

News / Local News

Hackers demand ransom after Westmount targeted by cyberattack: report

"I want to reassure all Westmounters that our teams are working seriously and diligently to remedy this situation," Mayor Christina M. Smith said.

Montreal Gazette

Published Nov 22, 2022 • 1 minute read

Join the conversation

CTV NEWS
MONTREAL

Joe Lofaro
CTVNewsMontreal.ca Digital Reporter
Follow | Contact

Updated Nov. 22, 2022 6:51 a.m. EST
Published Nov. 21, 2022 7:14 p.m. EST

Share

The City of Westmount confirmed Monday evening that it was hit with a cyberattack, which has caused a computer outage and disabled the city's email servers.

"The Information Technology Department is working with a leading external cybersecurity firm to determine the extent of the attack and how to re-establish our systems as quickly and efficiently as possible. The City's website is unaffected," read a statement on the city's website.

The cyberattack was first reported by La Presse, which said the hacker group Lockbit had gained access to 14 terabytes of data and demanded a ransom to be paid, otherwise the files would be published in two weeks.

The City of Westmount did not respond to multiple requests for comment from CTV News. At a council meeting early Monday evening, officials addressed the attack but did not confirm it was a ransomware style of cyberattack. They asked members of the public to communicate with the city via phone or in person at a service location.

"Cyberattacks are unfortunately becoming more and more prevalent and sophisticated in our society and, despite all the measures we put in place, public administrations are not completely immune to this sad reality. I want to reassure all Westmounters that our teams are working seriously and diligently to remedy this situation, and we will keep residents informed," said Westmount Mayor Christina M. Smith in a written statement.

A cybersecurity expert said the hacker group has exaggerated the size and scope of stolen data in the past, but may have started using smarter tactics.

Jacques Sauve, an analyst who helps businesses mitigate risks of cyberattacks, said in previous cases hackers would encrypt files after infiltrating a network and then demand a ransom.

"But then the customers got wise and they started doing good, solid backups. So when their data was encrypted, they would just restore and go, 'I'm not going to pay.' So the bad guys decided on a new tactic: let's steal the data first, then encrypt. So now we're looking at double extortion and this is most likely what's going to happen here," Sauve said.

Nouvelles

Cyberattaque contre Westmount – Mise à jour du 25 novembre 2022

25 novembre 2022

La Ville de Westmount compose toujours avec l'attaque informatique dont elle a été victime, et qui a été détectée le dimanche 20 novembre 2022.

Certains services offerts par la Ville ont été impactés, mais la plupart des activités et des services continuent à opérer. Les communications envoyées par courriel vers la Ville, interrompues ce lundi 21 novembre, sont en cours de rétablissement. Les résidents peuvent également contacter les différents services par téléphone (consultez le répertoire des Services) ou se rendre à un point de service.

Nouvelles

Cyberattaque contre la Ville de Westmount – Message de la mairesse

5 décembre 2022

(Allocution prononcée lors de la séance ordinaire du Conseil du 5 décembre 2022)

Chèr(e) résident(e)s

Je voudrais vous dire quelques mots au sujet de la cyberattaque dont notre Ville a été la victime. Tout d'abord, je veux vous dire que nous sommes aussi parfaitement conscients que cet événement peut susciter, à juste titre, des inquiétudes dans la communauté, et parmi nos employés(e)s. Les médias également veulent en savoir un peu plus sur notre situation par rapport à cette attaque. Tout ceci est parfaitement normal. Bien que de plus en plus fréquent dans nos sociétés, ce n'est pas un événement banal.

Mais c'est justement parce qu'il s'agit d'un événement particulièrement délicat et sérieux qu'il faut en gérer tous les aspects de façon stratégique et avec beaucoup de prudence, incluant l'aspect communicationnel.

Tout d'abord, je voudrais vous rappeler les faits. Le dimanche 20 novembre, la cyberattaque a été détectée par notre Service des technologies de l'information. L'attaque proviendrait du groupe criminel Lockbit 3.0. Ce groupe prétend avoir eu accès à une quantité importante de données de la Ville qui, pour l'essentiel, sont déjà de nature publique.

Bibliothèque publique de Westmount Public Library
Published by Lora Baiocco · November 20, 2022 ·

📌 Veuillez noter que les services en ligne ne sont pas disponibles en ce moment. Une mise à jour sera communiquée lorsque les services seront rétablis.

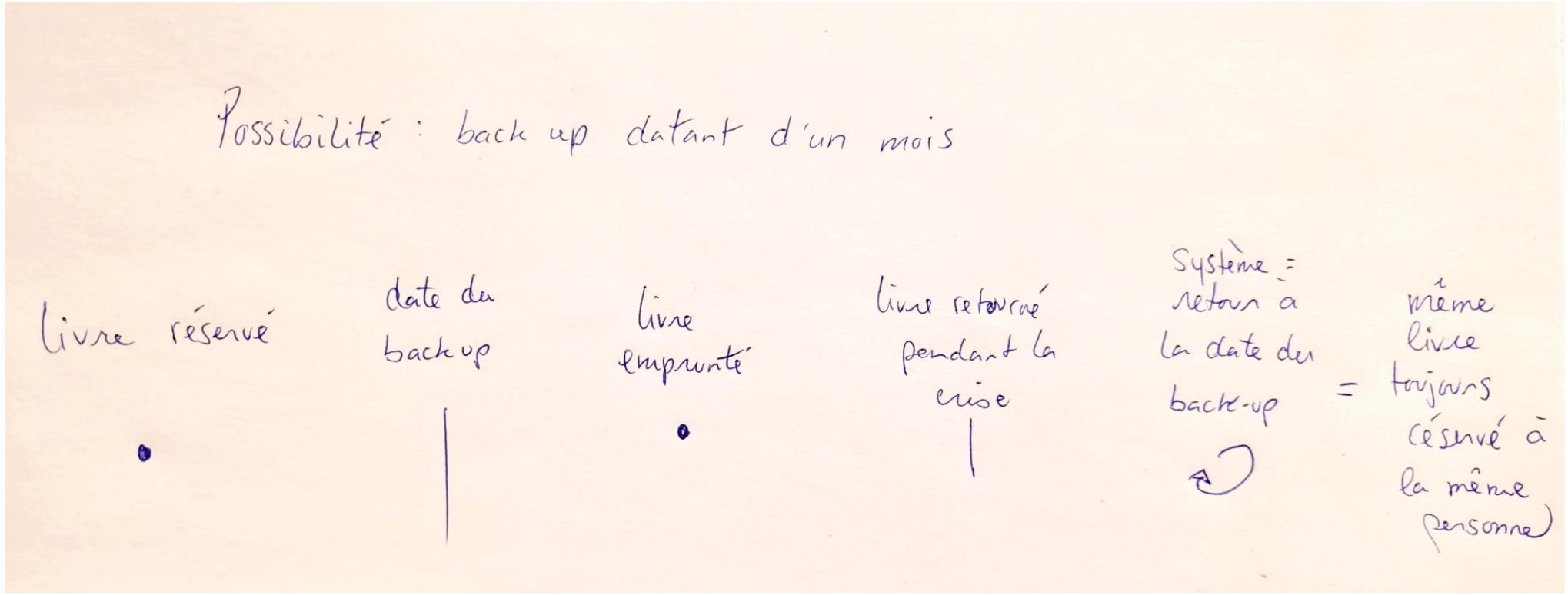
❌ Les services suivants sont affectés : site Web, comptes d'abonnés, système de réservation, et services en ligne.

Merci de votre compréhension.... See more

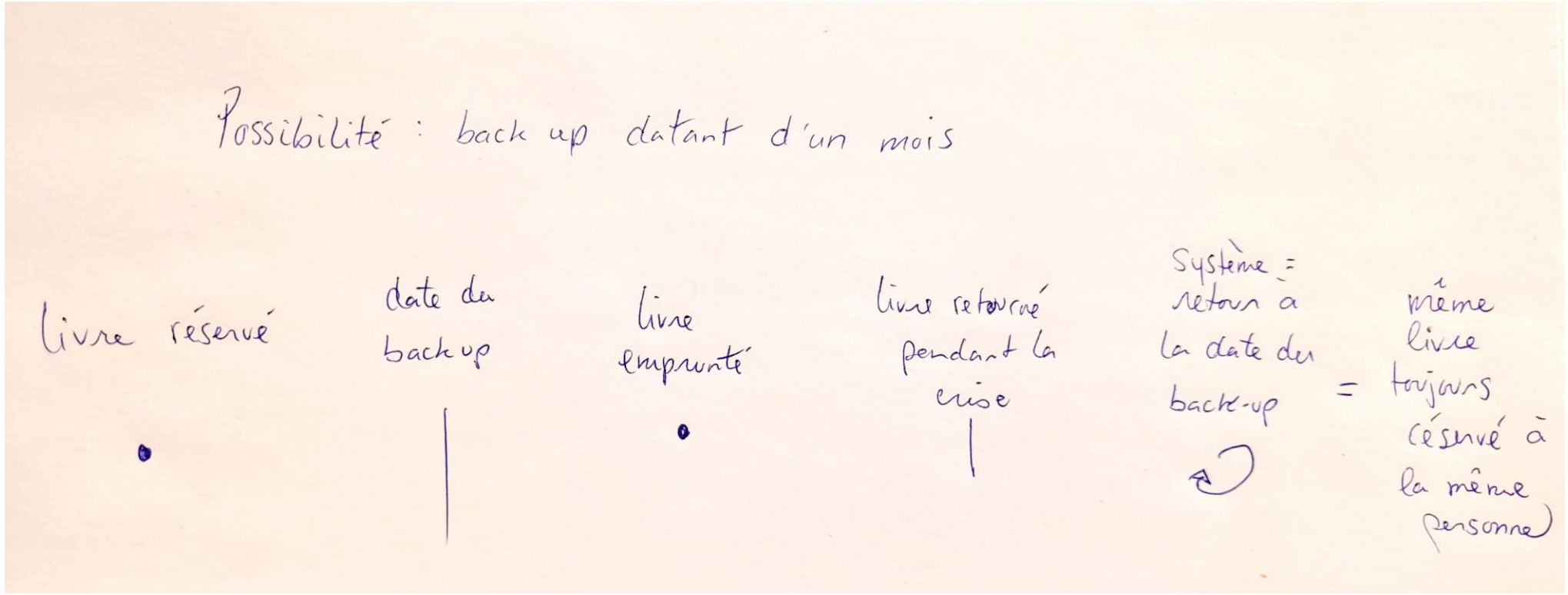
Planification et création de scénarios - Circulation

- Identification des problèmes potentiels
- Planification de la meilleure réponse à chaque problème
- Stratégies pour minimiser les problèmes additionnels

Planification et création de scénarios



Planification et création de scénarios



Planification et création de scénarios

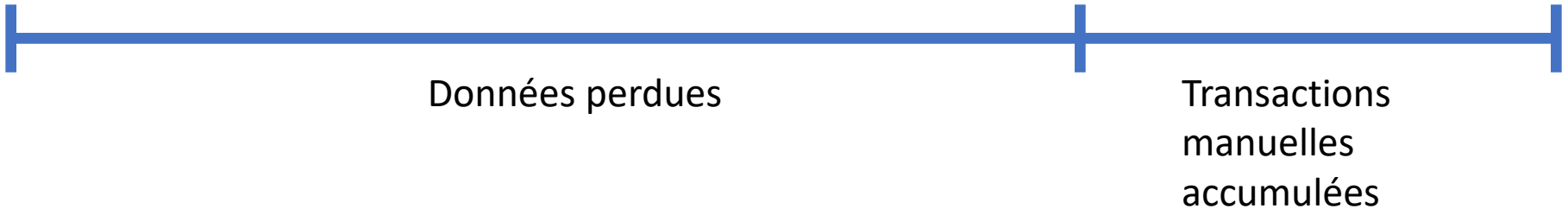
Type de transaction	Conséquence si la transaction est perdue	Action possible
Prêts	Document impossible à retracer à l'abonné	
	Document considéré encore réservé	
	Document considéré encore sur la tablette des réservations	
Retours	Document peut apparaitre encore sur la carte de l'abonné et faire atteindre le nombre maximum permis	Lever la limite maximale de prêts
	Document peut générer des amendes	Annulation de toutes les amendes
	Document sur la tablette avec le mauvais statut - impossible de savoir lesquels	Il faut rechercher les documents (rretournés après le dernier back-up mais avant la cyberattaque)
Renouvellements	Document peut paraitre en retard et générer amendes et avis	Annulation des amendes et suspension des envois d'avis
Nouvelles réservations	Les réservations ne sont plus enregistrées dans le SIGB	Nous disons aux abonnés que leur réservations doivent être faites à nouveau et que l'ordre de priorité n'a pas été conservé
Nouveaux abonnements	Ces abonnements n'existent plus	Il faut refaire les abonnements au fur et à mesure
	Des documents peuvent se trouver chez des gens dont le compte / abonnement n'existe plus	Espérer que les documents soient rendus
Renouvellement d'abonnements	Les abonnées ne peut plus accéder à leur compte en ligne car il est bloqué	Il faut renouveller les abonnements à nouveau
Documents catalogués	Des documents doivent être recatalogués, il faut trouver lesquels	Utiliser les factures récentes pour retracer les titres
	Certains documents sont retournés mais sont inconnus du SIGB	Retourner les documents au département de catalogage
Documents élagués	Le catalogue contient des notices pour des documents que nous n'avons plus	Un inventaire complet sera requis
Avis (retard, courtoisie, etc.)	Des avis générés par le SIGB et datant du back-up risquent d'être envoyés à nouveau	
	Des avis désuets risquent d'être envoyés	Supprimer les avis ayant été produits
Amendes payées	Des amendes déjà payées risquent d'apparaitre dans les comptes d'abonnés	Annuler les amendes existantes
Mises à jour d'informations personnelles (compte d'abonnés)	Les changements apportés aux numéros de téléphone, courriels, adresse, etc. sont perdus	Certains abonnés pourraient être injoignables
GÉNÉRAL	Les abonnés vont voir des information erronées dans leur compte	Afficher un avis dans le compte d'abonné, indiquant la présence probable d'informations erronées

Planification et création de scénarios

	Délai	Prêts	Retours	Renouvellements	Nouvelles réservations	Nouveaux abonnements	Renouvellements d'abonnement	Documents catalogués	Documents élagués
Par mois (estimé sur 30 jours)	1	14100	14000	4600	3500	200	460	750	100
Par jour (modifier nombre de jours)	15	7050	7000	2300	1750	100	230	375	50

Situations prioritaires identifiées en prévision du retour du système

- Traiter l’accumulation de retours et prêts
- Évaluer les dommages de toute perte de données (le nerf de la guerre)



Leçons apprises de la phase 1:

- Garder une liste locale ou imprimée des contacts importants (vendeurs de bases de données ou du SIGB, numéros de téléphone ou courriels personnels des employés)
- Avoir sous la main des appareils mobiles pour la communication interne et la gestion des médias sociaux
- Avoir une liste de tâches ‘’alternatives’’ pour occuper certains membres du personnel
- Être prêts à communiquer les conséquences

Phase 2: Récupération et atténuation

Nov. 30

Le SIGB est de nouveau fonctionnel

Nous pouvons maintenant voir dans le système qu’il manque 23 jours de données

- Ces données peuvent-elles être récupérées?
- Quelles tâches est-il possible d’effectuer sans causer des problèmes supplémentaires?
    - Téléphoner aux membres/ réservations
    - Trier les retours par date et identifier les documents devant retourner au catalogage


THE EDGE
PETER ROBINSON
TREVOR NOAH
BORN A CRIME


ROBIN BOOK CLUB
THE OCTOBER COUNTRY
Ray Bradbury
BRIDAL CHAIR
DOMINICANA
THE BINDING
BRIDGET COLLINS
TOM WOLFE
STEPHEN KING
Lisa Gerard
JACK CARR
IN THE BLOOD
The Deceptions
Brilasky
housebreaking
colleen hubbard
educated
TARA WESTOVER
CROOKED
AUSTIN
ONE BY ONE
Bloomsbury Girls
ROOSTER BAR
JOHN GRISHAM
Silva
THE AMERICAN HEIRESS
CROW LAKE
PAPIER CRÉATIF
DAVID NASH
LOUISE PENNY
ROKESBY
FATHOMS
Daniel Silva
A Death in Vienna
THE UNLIKELY SPY
DANIEL SILVA
Ireland
LE GUIDE DU LAUTO 2022
LANNUEL
ALEJANDRO ZAMBRA
CHILEAN PO

Autres actions

- Augmentation de la limite du nombre de prêts par carte
- Amendes pour toutes catégories de documents changées pour 0$
- Borne d’auto-prêt mise ‘’hors service’’
- Fonction de réservation désactivée pour le public
- Message de réponse courriel automatique
- Annulation de l’envoi des notices générées dans le SIGB
- Création de différents rapports système pour tenter de retracer des documents

Autres actions (suite)

- Désactivation des suspensions de compte (SIGB et fournisseurs/SIP2)
- Avis affichés sur le site Web et le compte d’abonné en ligne

Mise à jour concernant votre compte de bibliothèque

Il se peut que votre compte de bibliothèque ne soit pas à jour suite à la cyberattaque dont a été victime la Ville de Westmount le 20 novembre dernier.

Certaines transactions effectuées après le 28 octobre pourraient ne pas apparaître dans votre compte.

Vous pourriez voir :

- des documents dans votre compte que vous avez déjà retournés
- des documents que vous avez à la maison et qui ne figurent pas dans votre compte
- que votre position dans la file d'attente des réservations a changé ou a disparu
- que d'anciennes réservations apparaissent dans votre compte
- que votre abonnement a expiré bien que vous l'ayez renouvelé

Vous remarquerez peut-être également que vous ne pouvez pas faire de nouvelles réservations dans le catalogue.

Le personnel de la Bibliothèque s'efforce de mettre à jour votre compte le plus rapidement possible, mais il faudra un certain temps pour que ce travail y soit reflété.

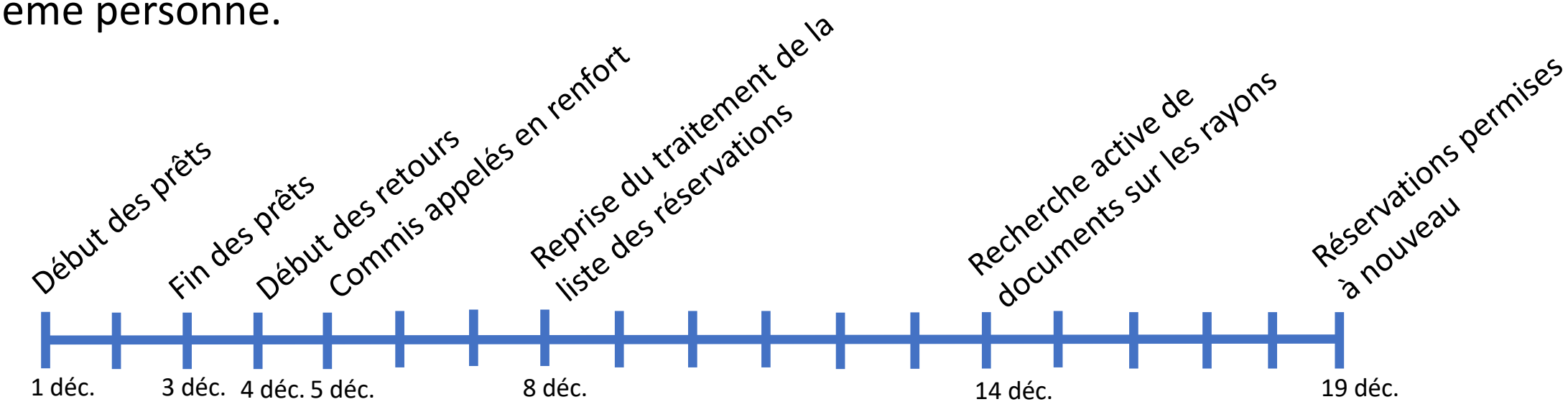
Nous voulons nous assurer que les informations figurant dans votre compte de bibliothèque soient exactes et, conséquemment, aucuns frais de retard ne seront facturés pendant que nous mettons les comptes à jour.

Nous vous remercions de votre patience et vous prions de nous excuser pour tout désagrément.

1er décembre

- Confirmation que les données ne peuvent pas être récupérées
- Les employés commencent à entrer les prêts manuels dans Vsmart

Traiter les prêts avant les retours permet de s'assurer qu'un document prêté et retourné pendant le fenêtre de 10 jours (phase 1 manuelle) ne sera pas prêté à la même personne.



23 jours de transactions perdues

- 11 000 prêts non enregistrés – éventuellement retournés ou perdus
- 11 000 retours non enregistrés – éventuellement retrouvés en rayon , retournés, ou perdus
- 3 500 renouvellements non enregistrés – retards visibles dans le compte des abonnés
- 2 600 réservations non enregistrées – perdues
- 150 nouveaux abonnements non enregistrés – doivent être refaits
- 350 renouvellement d'abonnements non enregistrées – doivent être renouvelés à nouveau
- 500 livres catalogués non enregistrés – Doivent être retrouvés et recatalogués
- 200 livres élagués non enregistrés – Un inventaire de la collection sera nécessaire

Leçons apprises de la phase 2:

- Connaitre à l’avance l’horaire de sauvegarde des données
- Demander à augmenter la fréquence si elle n’est pas satisfaisante
- Avoir à disposition un inventaire des systèmes et leurs emplacements (noms des serveurs ou adresses IP)
- Faire des sauvegardes locales ou infonuagiques de documents importants

Phase 3: Adaptation et Ajustements continus

Aspect public et circulation:

- Anomalies dans les comptes d'abonnés

Dans les coulisses:

- Accès VPN pour notre vendeur de SIGB désactivé (pas de support possible)
- Double authentification implémentée (compliqué pour les postes de travail partagés)
- Changements apportés par les TI causent des délais ou des rebonds des avis de courtoisie
- Mises à jour du pare-feu (Impact sur l'accès aux services externes, livres numériques, etc.)

Leçons apprises de la phase 3:

- L’importance de rencontrer le département TI pour leur présenter les activités et particularités des systèmes de la Bibliothèque
- Insister pour que tout changement lié aux mesures de sécurité, serveurs, adresses IP, etc. soient communiqués en avance à la bibliothèque.

La situation est-elle rétablie?

Type de transaction	Conséquence si la transaction est perdue	Action possible
Prêts	Document impossible à retracer à l'abonné	
	Document considéré encore réservé	
	Document considéré encore sur la tablette des réservations	
Retours	Document peut apparaitre encore sur la carte de l'abonné et faire atteindre le nombre maximum permis	Lever la limite maximale de prêts
	Document peut générer des amendes	Annulation de toutes les amendes
	Document sur la tablette avec le mauvais statut - impossible de savoir lesquels	Il faut rechercher les documents (rretournés après le dernier back-up mais avant la cyberattaque)
Renouvellements	Document peut paraitre en retard et générer amendes et avis	Annulation des amendes et suspension des envois d'avis
Nouvelles réservations	Les réservations ne sont plus enregistrées dans le SIGB	Nous disons aux abonnés que leur réservations doivent être faites à nouveau et que l'ordre de priorité n'a pas été conservé
Nouveaux abonnements	Ces abonnements n'existent plus	Il faut refaire les abonnements au fur et à mesure
	Des documents peuvent se trouver chez des gens dont le compte / abonnement n'existe plus	Espérer que les documents soient rendus
Renouvellement d'abonnements	Les abonnées ne peut plus accéder à leur compte en ligne car il est bloqué	Il faut renouveller les abonnements à nouveau
Documents catalogués	Des documents doivent être recatalogués, il faut trouver lesquels	Utiliser les factures récentes pour retracer les titres
	Certains documents sont retournés mais sont inconnus du SIGB	Retourner les documents au département de catalogage
Documents élagués	Le catalogue contient des notices pour des documents que nous n'avons plus	Un inventaire complet sera requis
Avis (retard, courtoisie, etc.)	Des avis générés par le SIGB et datant du back-up risquent d'être envoyés à nouveau	
	Des avis désuets risquent d'être envoyés	Supprimer les avis ayant été produits
Amendes payées	Des amendes déjà payées risquent d'apparaitre dans les comptes d'abonnés	Annuler les amendes existantes
Mises à jour d'informations personnelles (compte d'abonnés)	Les changements apportés aux numéros de téléphone, courriels, adresse, etc. sont perdus	Certains abonnés pourraient être injoignables
GÉNÉRAL	Les abonnés vont voir des information erronées dans leur compte	Afficher un avis dans le compte d'abonné, indiquant la présence probable d'informations erronées

Albrecht, S. (2023). **Keeping libraries safe from DIGITAL ATTACKS**. *Computers in Libraries, 43*(5), 8-12.

Enis, M. (2022). **Held for ransom: Ransomware attacks are on the rise, and several libraries have been hit by opportunistic criminals**. *Library Journal, 147*(4), 22.

Fichter, D., & Wisniewski, J. (2016). **Hidden dangers threatening your library website.** Online Searcher, 40(5), 66-68.

Merci!

lbaiocco@westmount.org

jbouchard@westmount.org