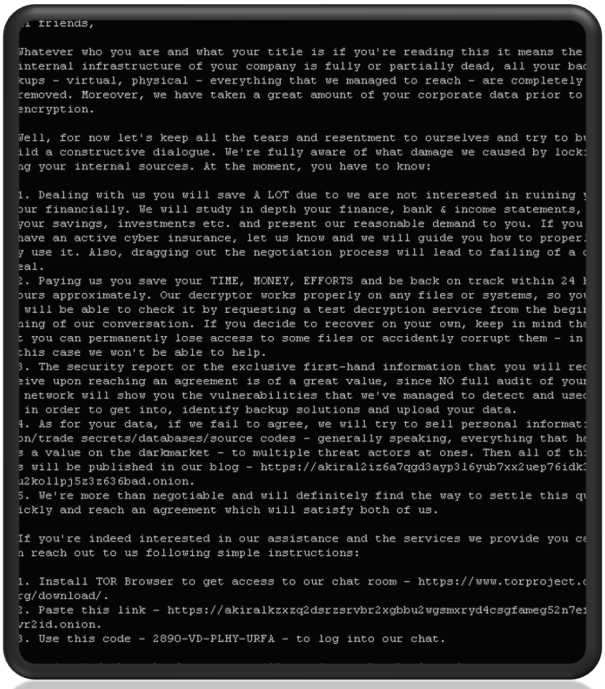
Berliner Hochschule für Technik

29. April 2024

Post-Mortem-Bericht[1] zum Akira-Cyberangriff

Verantwortlich: Präsidium der Berliner Hochschule für Technik
Autoren: Prof. Dr. Peter Tröger, Thomas Pehle
Reviewer: Prof. Dr. Zbigniew Jerzak
Status: Genehmigt



[1] *Wir folgen einem schuldlosen Postmortem-Prozess. Diese Vorlage basiert auf Postmortem Culture: Learning from Failure.*

Studiere Zukunft

Zusammenfassung

Am 20. Februar 2024 wurden zentrale Server der Berliner Hochschule für Technik (BHT) durch die Ransomware-Gruppe Akira heruntergefahren und teilweise verschlüsselt. Der Angriff wurde durch den resultierenden Ausfall der zentralen IT-Dienstleistungen entdeckt und kurz danach gestoppt, indem die Internetanbindung des gesamten Campus durch das Hochschulrechenzentrum (HRZ) unterbrochen und alle relevanten Server heruntergefahren wurden. Die Angreifer erlangten den Zugriff auf das Netzwerk der BHT - nach aktuellen Erkenntnissen – zwischen dem 14. Februar und dem 20. Februar 2024.
Aktuell müssen aufgrund des Angriffs verschiedene Server-Dienste im HRZ wiederhergestellt und gehärtet werden. Parallel müssen die von den Angreifern ausgenutzten Schwachstellen im Netzwerk der Hochschule systematisch und nachhaltig behoben werden. Da eine forensische Analyse kein vollständiges Bild des Angriffsverlaufs liefern kann, ist eine Überprüfung sämtlicher IT-Geräte der Hochschule auf Spuren der Angreifer erforderlich, bevor ein großflächiger Zugriff auf das Internet wieder erlaubt werden kann. Die Wiederherstellungsmaßnahmen für die IT-Dienstleistungen der Hochschule sind zum Zeitpunkt der Erstellung dieses Dokuments noch nicht abgeschlossen.
Der geschätzte finanzielle Verlust lässt sich derzeit nur schwer beziffern. Es wird angenommen, dass die Zahl der neu eingeschriebenen Bachelor- und Masterstudierenden im Sommersemester 2024 durch den Vorfall verringert wurde, was sich indirekt auf den Haushalt der Hochschule auswirkt. Ein weiterer bedeutender Kostenfaktor sind die technischen und personellen Ressourcen, die von Hochschulrechenzentrum, Studienverwaltung, Studienberatung, Dekanaten, AStA und anderen Organisationseinheiten zur Bewältigung des Vorfalls bereitgestellt werden mussten. Es wird erwartet, dass verschiedenste zentrale IT-Projekte - unabhängig von ihrer Dringlichkeit - aufgrund des Vorfalls um mindestens 3 Monate verschoben werden müssen. Beispiele hierfür sind die gesetzlich geforderte Einführung der E-Rechnung, die Erneuerung der Druckerlandschaft oder die hochschulweit notwendige Aktualisierung auf Windows 11. Die Arbeitsfähigkeit der Labore, Forschungsgruppen und Lehrkräfte wird mindestens für die nächsten 6 Monate stark beeinträchtigt sein.
Der Vorfall hat gezeigt, dass zum Thema IT-Betrieb im HRZ und in den über 70 Laboren der Hochschule zu viele unbesetzte Stellen und teilweise überfordertes Personal existieren. Dadurch geraten komplexe Fragen der IT-Sicherheit im Alltag zu schnell in den Hintergrund. Dies bezieht sich vor allem auf die Entwicklung von Bedrohungsmodellen, auf die darauf basierenden Risikoabschätzungen und auf die Entwicklung von gezielten Gegenmaßnahmen. Somit wird, trotz des hohen Grundniveaus der IT-Sicherungsmaßnahmen in den Kernsystemen des HRZ, die Abwehrfähigkeit der Hochschule in ihrer Gesamtheit aktuell immer schwächer, da die Qualität der Angriffe weiter steigt. Vor dem Hintergrund des erfolgreichen Angriffs ist es somit von großer Bedeutung, dass zukünftig klarere organisatorische und strengere technische Maßnahmen zur Steigerung der Cyber-Resilienz entwickelt und umgesetzt.
Die technischen Details des vorliegenden Berichts basieren auf einer forensischen Analyse der Firma Trend Micro [TMIRT], welche zwischen dem 20. Februar 2024 und 5. März 2024 als direkte Reaktion auf den Ausfall durchgeführt wurde.

Ursachenanalyse

Der Ausfall der zentralen IT-Dienstleistungen der BHT am 20.2.2024, welche bis heute andauert, wurde durch eine Folge von ungeplanten Ereignissen ausgelöst. Der Zusammenhang dieser Ereignisse wird im Sinne einer Fehlerausbreitungskette (*error propagation chain*) im Folgenden dargestellt.

Warum sind die zentralen IT-Dienstleistungen der BHT ausgefallen?

→ Eine professionell agierende Gruppe von Cyberkriminellen (Akira) verschaffte sich Zugang zur zentralen, virtualisierten Server-Infrastruktur im HRZ, welche einem Großteil der zentralen Dienstleistungen (Moodle, E-Mail, Webseite, Laborserver, ...) zu Grunde liegt. Die Angreifer stoppten einen Großteil der zentralen Server, um anschließend die zugehörigen virtuellen Festplatten verschlüsseln zu können.

Warum hatten die Angreifer die Möglichkeit, die Server im Virtualisierungscluster des HRZ herunterzufahren?

→ Die Angreifer hatten die administrativen Nutzungsrechte eines HRZ-Mitarbeiters zur Verfügung. Nach aktueller Sachlage wurde dies durch das Auslesen des Arbeitsspeichers eines einzelnen HRZ-Servers erreicht.

Warum war es für die Angreifer möglich, den Arbeitsspeicher eines HRZ-Servers auszulesen?

→ Die Angreifer hatten auf mehreren Windows-Servern der BHT den Zugang zu den jeweiligen lokalen Administrator-Konten erlangt. Auf dem konkreten Server des HRZ war es damit möglich, die Anmeldeinformationen des betroffenen HRZ-Mitarbeiters auszulesen, vermutlich aus einer parallel laufenden Remote Desktop (RDP)-Sitzung.

Warum war es für die Angreifer möglich, sich auf Windows-Servern der Hochschule mit lokalen administrativen Accounts anzumelden?

→ Zum Zeitpunkt des Angriffs war es lokalen Administratorkonten auf Windows-Servern der Hochschule erlaubt, sich direkt über das Netzwerk per RDP anzumelden. Ein physischer Zugang war somit unnötig. Die lokalen Administrator-Konten auf den Windows-Servern der Domäne hatten zum Zeitpunkt des Angriffs dabei keine reguläre Passwort-Rotation, und unterlagen auch nicht den zentralen Passwort-Richtlinien bzgl. der Anzahl der Fehleingaben bei Authentifizierungen. Vor diesem Hintergrund war es möglich, automatisierte Brute-Force-Angriffe auf lokale Administrator-Konten innerhalb des BHT-Netzwerks per RDP über mehrere Tage durchzuführen.

Warum war es für Angreifer möglich, RDP-Sitzungen im Netzwerk der Hochschule über mehrere Tage probeweise zu authentifizieren und interaktive Anmeldeversuche innerhalb des BHT-Netzwerkes auf HRZ-Servern durchzuführen?

→ Die Angreifer hatten in verschiedenen Laboren der Hochschule die dortigen Windows-Computer angegriffen und diverse Accounts und Computer

übernommen. Somit war es den Angreifern möglich, auf diesen Labor-Computern diverse Werkzeuge zu installieren und von dort Brute-Force-Angriffe auf andere Labore und HRZ-Server und deren lokale Administrator-Konten auszuführen. Der grundsätzliche Zugriff von Labor-Rechnern auf Server-Freigaben des HRZ ist dabei Teil der regulären Dienstleistungen.

Warum konnten die Angreifer Zugriff auf Labor-Server und deren lokale Accounts erlangen?

→ Die Angreifer nutzten verschiedene RDP-Freigaben in den Firewalls der Hochschule, welche für Personen mit VPN-Einwahl den direkten Zugriff auf Windows-Server in Laboren erlaubten. Die lokalen Konten wurden durch XXX[2] übernommen.

Warum konnten die Angreifer auf RDP-Freigaben von Labor-Servern zugreifen, welche nur aus dem VPN erreichbar sind?

→ Die Angreifer hatten Zugriff auf einen studentischen Campus-Account mit Passwort erlangt, und konnten somit diese Daten für einen regulären Zugang zum BHT-Netzwerk per VPN nutzen.

Warum war es für Angreifer möglich, sich mit einem übernommenen studentischen Campus-Account und Passwort einzuloggen?

→ Weil die BHT zum Zeitpunkt des Angriffs keine Mehrfaktor-Authentifizierung für die Einwahl über VPN im Einsatz hatte.

Detaillierter Verlauf

Die folgenden Ausführungen zum detaillierten Verlauf des Angriffs basieren zum größten Teil auf der forensischen Analyse der Firma Trend Micro [TMIRT]. Es handelt sich hier um eine Zusammenstellung von Indizien, welche durch die noch laufenden Scans aller Systeme der Hochschule fortlaufend ergänzt werden.

Zeitstempel (UTC)	**Ereignis**
<unbekannter Zeitpunkt>	Die Angreifer erlangten zu einem unbekannten Zeitpunkt Zugang zum Nutzernamen und Passwort eines studentischen Campus-Accounts („account1“), welcher regulär für die Einwahl in das BHT-Netzwerk über *Virtual Private Network (VPN)* genutzt werden kann.
TAG 1 - Mittwoch	
2024-02-14 05:39:00	Die erste nachvollziehbare Angreifer-Aktivität findet im BHT-Netzwerk statt. Die Angreifer fragen im LDAP die öffentlich verfügbaren Namen der

[2] *Die Unkenntlichmachung bestimmter Teile dieses Berichts („XXX“) basiert auf einer Empfehlung des Informationssicherheitsbeauftragten der Berliner Hochschule für Technik.*

	Campus-Accounts und der vom HRZ betreuten Endgeräte ab. Der Zugriff auf diese Informationen ist aus dem BHT Netzwerk erlaubt und für den Normalbetrieb notwendig.
2024-02-14 13:10:15	Die Angreifer suchen durch Scannen des internen Hochschulnetzwerks gezielt nach *Server Message Block (SMB)* Protokoll-Freigaben und führen dort probeweise Anmeldungen mit bekannten Standardpasswörtern für lokale Nutzer durch.
2024-02-14 13:15:48	Erste erfolgreiche Anmeldung aus dem VPN auf einem Windows Server im Labor1 mit einem lokalen Account („XXX“) über das *Remote Desktop Protocol (RDP).* Die Angreifer lesen anschließend Nutzernamen und Passwörter aus XXX aus. Die Angreifer führen weitere Scans des Netzwerks durch und analysieren vorhergehende ausgehende RDP Verbindungen (Nutzername, Ziel-Host), um weitere Angriffsziele zu ermitteln.
2024-02-14 13:22:44	Weitere erfolgreiche Anmeldung aus dem VPN auf einem weiteren Windows Server des gleichen Labors mit einem lokalen Account („XXX“) über das *Remote Desktop Protocol (RDP)*. Die Angreifer lesen erneut Nutzernamen und Passwörter aus XXX aus.
2024-02-14 13:27:26	Die Angreifer nutzen „lab1-pc1“, um weitere Scans des Netzwerks durchzuführen. Hierfür wird das Programm „XXX“ eingesetzt. Der auf der Maschine installierte Virenscanner „Windows Defender“ erkennt diesen Vorgang und meldet eine entsprechende Warnung des Typs *„XXX“*. Die Angreifer deaktivieren diese Warnung auf dem Computer und setzen ihre Tätigkeit fort. Die Windows Defender meldet diese Vorgänge nicht weiter, womit sie keine Alarmierung beim HRZ oder im Labor auslösen.
2024-02-14 13:57:56	Erfolgreiche Anmeldung aus dem VPN auf einem Windows-Server im Labor2 („lab2-pc1“) mit einem lokalen Account („XXX“), wieder über das *Remote Desktop Protocol (RDP).* Die Angreifer installieren dort die Backdoor „XXX“. Zum Zeitpunkt der forensischen Analyse konnten keine Verbindungen dieser Backdoor mit C&C-Servern im Internet nachgewiesen werden.
2024-02-14 14:34:19	Erfolgreiche Anmeldung von „lab1-pc1“ in der Windows-Domäne der Hochschule mit einem übernommenen Campus Account („account2“). Es ist davon auszugehen, dass die Zugangsdaten im Rahmen der vorherigen Aktivitäten ermittelt wurden.
TAG 2 - Donnerstag	
2024-02-15 11:10:22	Die Angreifer nutzen ihren Zugang auf „lab1-pc1“ über die VPN-Verbindung, um mit Hilfe der Zugangsdaten von „account2“ den Zugriff auf zentrale Dateifreigaben zu testen. Im Rahmen der initialen Forensik konnten mindestens erfolgreiche Anmeldungen an folgenden Systemen festgestellt werden: „hrz-computer1“, „hrz-computer2“, „hrz-computer3“, „hrz-computer4“ und „lab3-pc1“. Auf den Dateifreigaben der HRZ-Server führt das Rechtemanagement für Campus-Accounts dazu, dass die Angreifer keinen Zugriff auf relevante Daten erlangen.

2024-02-15 12:03:06	XXX
TAG 3 - Freitag	
2024-02-16 09:46:30	Die Angreifer melden sich erneut mit einem lokalen Konto über RDP bei einem Laborrechner an („XXX“) und führen erneut Netzwerk-Scans mit verschiedenen Werkzeugen durch, welche sie direkt ohne Ablage im Dateisystem herunterladen und ausführen. Die Angreifer versuchen auch die Sicherheitslücke XXX auszunutzen, um durch eine Schwachstelle in XXX verschlüsselte Anmeldedaten aus der XXX selbst auszulesen. Es wird vermutet, dass zu diesem Zeitpunkt massive Brute-Force-Angriffe auf lokale Administrator-Konten bei verschiedenen Servern unternommen werden. Diese bleiben aber unentdeckt.
2024-02-16 11:38:42	Die Angreifer melden sich mit einem lokalen Administratorkonto über RDP auf „hrz-computer2“ an. Die Maschine gehört zu den Kernsystemen des HRZ, und bietet nachgelagerte Dienste für das ERP-System der Hochschule an. Es ist nicht restlos geklärt, wie die Angreifer das zugehörige Administratorpasswort erlangen konnten. Aufgrund des Betreuungsstatus der Maschine (sollte 2024 abgelöst werden, Administrator seit mehreren Jahren nicht mehr an der Hochschule, nur noch Sicherheitsaktualisierungen) wird momentan davon ausgegangen, dass das Passwort per Brute Force im vorherigen Schritt ermittelt wurde. Die Angreifer versuchen, weitere (temporäre) Zugangsdaten für die Domäne (Kerberos Tickets) aus XXX auszulesen. Falls vorhanden, ermöglichen solche temporären Zugangsdaten eine Anmeldung ohne Kenntnis des Passworts.
2024-02-16 11:54:49	Die Angreifer melden sich mit dem lokalen Administratorkonto über RDP auf „hrz-computer3“ und „hrz-computer4“ an. Die Recherche des HRZ ergab, dass „hrz-computer2“, „hrz-computer3“ und „hrz-computer4“ vom ausgeschiedenen Administrator mit dem gleichen schwachen Passwort geschützt wurden. Auch hier erfolgt die Suche nach Kerberos-Tickets XXX. Ein Zugriff auf personenbezogene Daten, mit denen innerhalb der nachgelagerten ERP-Fachanwendungen gearbeitet wird, kann nach Stand der Forensik ausgeschlossen werden, da diese zusätzliche anwendungsinterne, separate Authentifizierungen verwenden. Diese sind nicht direkt mit der zentralen Benutzerverwaltung im Active Directory gekoppelt. Die Nutzerdatenbanken der Fachanwendungen befinden sich zudem nicht auf den übernommenen Computern.
2024-02-16 14:21:50	Die Angreifer führen die erste nachvollziehbare Nutzung eines administrativen HRZ-Accounts („account3“) in der Domäne durch. Die Angreifer erstellen mit Hilfe der Zugangsdaten eine Kopie des Active Directory, inkl. der verschlüsselt abgelegten Passwörter. Nach aktuellen Verständnis erlangen die Angreifer Zugriff auf den Account, indem auf „hrz-computer2“ mit Hilfe des lokalen Administrator-Kontos der gesamte Hauptspeicher ausgelesen und auf gehashte Passwörter und Token untersucht wurde.

TAG 4 - Samstag	
keine Aktivität	
TAG 5 - Sonntag	
2024-02-18 20:30:00	Das Präsidium erhält eine unspezifische Warnung der deutschen Sicherheitsbehörden zu einem bevorstehenden Cyberangriff auf die Hochschule. Es werden keinerlei technische Details oder Indizien mitgeteilt. Das Hochschulrechenzentrum trennt am gleichen Abend das zentrale Backupsystem physisch vom Netzwerk und führt eine routinemäßige Überprüfung der Überwachungssysteme durch. Da zu diesem Zeitpunkt XXX, und die eingesetzte Vielfalt von Virenscannern im Umfeld der Hochschule keine akkumulierte zentrale Datensammlung vornimmt, wird keine direkte Bedrohung ausgemacht. Aus den beim Angriff betroffenen Laboren liegt zu diesem Zeitpunkt keine Meldung vor.
TAG 6 - Montag	
2024-02-19 08:28:30	In dieser Phase des Angriffs konzentrieren sich die Angreifer auf die Ermittlung von Daten, die verschlüsselt werden können. Die Angreifer melden sich erneut mit einem lokalen Konto über RDP an einem Laborrechner an („XXX“). Sie öffnen mit den bisher übernommenen Accounts eine Vielzahl von Netzwerkfreigaben auf mehreren Rechnern. Weiterhin werden zusätzliche Netzwerk-Scans durchgeführt. Das Dateiberechtigungskonzept der Freigaben verhindert auch hier wieder signifikanten Datenabfluss.
2024-02-19 09:11:38	Die Angreifer unternehmen weiterhin Versuche, sich über RDP vom „lab2-pc1“ aus auf anderen Rechnern per RDP anzumelden. Die Aktivitäten beschränken sich dabei auf Labor1.
2024-02-19, nachmittags	Das HRZ holt die Indizien der deutschen Sicherheitsbehörden persönlich auf einer gebrannten CD-ROM ab und wertet diese aus, nachdem ein Laufwerk organisiert wurde. Ein Zusammenhang zu den Aktivitäten der Angreifer ist nicht ersichtlich.
TAG 7 – Dienstag	
2024-02-20 06:54:24	In dieser letzten Phase des Angriffs konzentrieren sich die Angreifer auf Verschlüsselung von Daten. Die Angreifer melden sich über VPN und RDP an „lab1-pc2“ und ermitteln erneut die erreichbaren Netzwerkfreigaben. Danach wird ein erster Versuch der Verschlüsselung auf dem Rechner „lab1-pc2“ mit der Akira-Verschlüsselungssoftware gestartet, der jedoch aufgrund eines Absturzes des Verschlüsselungsprogramms nicht erfolgreich ist.
2024-02-20 07:20:56	Die Angreifer melden sich über RDP an „hrz-computer1“ mit „account3“ an.
2024-02-20 07:23:30	Die Angreifer melden sich mit „account3“ auf „hrz-vmhost1“ an. Dieser Rechner ist Teil der zentralen Virtualisierungsumgebung, auf der die

	meisten zentralen Server der Hochschule betrieben werden.
2024-02-20 07:23:51	In Vorbereitung eines weiteren Verschlüsselungsverfahrens werden SSH-Server auf „hrz-vmhost2“ und „hrz-vmhost15“ gestartet.
2024-02-20 07:29:42	Die Angreifer melden sich mit „account3“ auf „hrz-vmhost2“ an.
2024-02-20 07:33:25	Die Angreifer nutzen den Zugang zum Virtualisierungscluster, um insgesamt 252 virtualisierte Rechner auszuschalten. Die Deaktivierung der Server führt zu einer Vielzahl von Meldungen in den Alarmsystemen des HRZ.
2024-02-20 07:39:48	Die Angreifer beginnen damit, die virtuellen Festplatten der heruntergefahrenen Server zu verschlüsseln. Dies erfolgt interaktiv über die SSH-Zugänge in den Virtualisierungscluster.
2024-02-20 08:17:00	Nach Analyse der Alarmierungen beginnt das Hochschulrechenzentrum mit der Abschaltung aller IT-Dienste, der Deaktivierung von "account3" und der Außenanbindung der Hochschule. Die Verschlüsselung der Serversysteme wird damit gestoppt und der weitere Zugriff der Angreifer unterbunden.

Wiederherstellungsmaßnahmen

Mit Hinblick auf den langjährigen Personalmangel in allen Bereichen der IT wird die Wiederherstellung der gehärteten Dienste noch Monate in Anspruch nehmen. Die folgende Aufzählung muss daher als Zwischenstand zum Zeitpunkt der Erstellung des Dokuments gewertet werden.

Zeitstempel	**Maßnahmen**
2024-02-20, vormittags	Trennung des gesamten BHT-Netzwerks vom Internet
2024-02-20, abends	Beginn der forensischen Analyse durch das TrendMicro Incident Response Team und das HRZ, Bildung des Krisenstabs
2024-02-22, vormittags	Abfrage von anonymisierten Datenverkehrsstatistiken beim DFN zur Analyse potentieller Datenabflüsse
2024-02-22	Inbetriebnahme der Notfallwebseite
2024-02-22, abends	Inbetriebnahme der im Rahmen des Vertrags gelieferten *Deep Discovery Inspection*-Appliance der Firma Trend Micro zur Verfolgung der Angreifer
2024-02-27	Zurücksetzung der gesamten Windows-Domäne auf den Stand vom 13.2.2024 aus dem zentralen Backup
2024-02-29, mittags	Zurücksetzung aller Passwörter für BHT-Campus-Account in der Domäne.

2024-03-02	Erste Version des Online-Formulars zur selbständigen Passwortrücksetzung
2024-03-04	Erste methodische Tests für die optimale Durchführung von Scans von Laborcomputern.
2024-03-05	Ende der forensischen Analyse durch das TrendMicro Incident Response Team.
2024-03-05	Beginn der Scans der Computer in der Verwaltung durch HRZ-Mitarbeiter
2024-03-11	Test des Verfahrens zum Scan von Laboren durch zusätzlich gewonnene Multiplikatoren
2024-03-11	Beginn des Versands von Briefen an ca. 13000 Studierende zur Passwortrücksetzung
2024-03-14	Beginn des breitflächigen Scans der Labore im Feld und Start von Schulungen weiterer Multiplikatoren
2024-03-18	Wiederherstellung erster IT-Dienste: Polli, Moodle (Kernsystem), Prüfungsportal, E-Mail, Shibboleth-Auth, Netzlaufwerke, Mach, IT-Dokumentation
2024-03-18	Wiederherstellung der BHT-Internetpräsenz
2024-03-25	Beginn separater Sprechstunden im HRZ-Servicebüro zur Unterstützung beim Passwort-Reset

Gewonnene Erkenntnisse

Was hat gut funktioniert?

Grundlegende Absicherung für BHT-Systeme im Internet
Der Angriff von Akira basierte auf der initialen Verfügbarkeit von gültigen Anmeldedaten. Ein alternativer Angriffsvektor auf im Internet stehende Systeme des HRZ, insbesondere auf die VPN-Einwahl, kann nach aktueller Sichtweise mit hoher Sicherheit ausgeschlossen werden. Die im Internet zugreifbaren Systeme, zumindest auf Seiten des HRZ, waren zum Zeitpunkt des Angriffs auf einem aktuellen Software-Stand und zeigten keine Anzeichen von Angriffsversuchen. Die Sicherheitslücke bestand hier ausschließlich im übernommenen Campus-Account.
Eine Übernahme von Campus-Accounts in der Windows-Domäne durch Ausprobieren des Passworts (*brute force*) ist weiterhin als unwahrscheinlich anzusehen, da Anmeldungen mit dem BHT Campus-Account nur eine beschränkte Anzahl von Fehlversuchen zulassen. Als weitere Sicherungsmaßnahme sind die minimale Anzahl von Zeichen und die Variabilität der Zeichen in den letzten Jahren durch das HRZ kontinuierlich verstärkt worden. Dies schließt auch die Prüfung eines gewählten Passworts gegen Datenbanken bekannter Hacks ein. Angreifbare Accounts existierten hier bisher ausschließlich in Form von lokalen Administrator-Konten, sowie durch XXX.

Berechtigungskonzept für Windows-Laufwerke
Die Berechtigungen des übernommenen „account2“ auf den Systemen des HRZ beschränkten sich auf die regulären Zugriffsrechte von Labor-Mitarbeitenden der Hochschule. Dadurch waren - trotz erfolgreicher Anmeldung - keine sensiblen Daten zugänglich. Die Server waren mit den neuesten Sicherheitsupdates versehen, sodass über die Berechtigungen von „account2“ hinaus kein weiterer Zugriff möglich war. Dies führt nach Analyse der Forensiker bei Trend Micro zu der Erkenntnis, dass mit sehr hoher Wahrscheinlichkeit kein signifikanter Datenabfluss aus den Systemen des HRZ stattfand. Diese beschränkten sich lediglich auf Labor1 und Labor2, welche (jeweils nach eigener Aussage) keine kritischen Daten vorhielten.
Der administrative Account „account3“ hatte gemäß der Richtlinien des HRZ keinen direkten Zugriff auf kritische Dateifreigaben, womit eine Datenexfiltration vermutlich erschwert wurde.

Backup
Die Backup-Zyklen und -Methoden des HRZ haben sich als zuverlässig erwiesen. Der Aufbau einer entkoppelten Lösung mit separaten, robusten Passwörtern erwies sich als angemessen und sinnvoll. Durch die regelmäßigen Wiederherstellungsübungen war das HRZ-Team gut auf das Wiederherstellungsszenario für verschlüsselte Server vorbereitet. Testsysteme und temporäre Installationen wurden bewusst nicht gesichert, dies stellte jedoch keinen Verlust dar. Für Labore, welche ihre virtuellen Maschinen im HRZ betreiben, war ebenfalls eine direkte Wiederherstellung aus dem Backup möglich und fand zeitnah statt.

Die Mehrheit der verschlüsselten Server war im Backup vorhanden, und konnte somit zeitnah wiederhergestellt werden. Einige Systeme, insbesondere Appliances, wurden aus Kapazitätsgründen bewusst aus dem Backup ausgeschlossen, da ein Neu-Aufsetzen dieser Rechner als genauso effizient eingeschätzt wurde. Ein typisches Beispiel sind Worker-Knoten für Opencast, welche durch Neuinstallation und Klonen der virtuelle Maschine schnell wiederherstellbar sind.
Eine einstellige Anzahl von Server konnte aus dem Backup nicht wiederhergestellt werden, da im Rahmen einer Aktualisierung die notwendige Anpassung der Backup-Pläne vergessen wurde. Dies führte zu verlängerten Wiederherstellungszeiten, da die Systeme komplett neu aufgesetzt werden mussten. Es zeigte sich jedoch, dass der Einsatz von automatisierten Installationen und Konfigurationen durch Ansible äußerst hilfreich ist und die Systeminbetriebnahme dadurch erheblich beschleunigt wird. Der zunehmende Tendenz zu *Infrastructure as Code* im HRZ hat sich hier also indirekt bewährt.

Reaktionszeiten
Die Reaktion des HRZ auf den erkannten Ausfall der IT-Systeme erfolgte zeitnah und professionell. Der am gleichen Tag einberufene Krisenstab koordinierte die notwendigen Maßnahmen zwischen Präsidium und HRZ auf eine - für beide Seiten - zufriedenstellende Art und Weise, und sorgte für eine zügige Kommunikation der Umstände nach Außen.

Was hat schlecht funktioniert?

VPN Authentifizierung
Eine fehlende Mehrfaktor-Authentifizierung (MFA) bei der VPN-Einwahl ermöglichte es den Angreifern, nach der Übernahme eines Campus-Accounts in das BHT-Netzwerk unbemerkt einzudringen. Dies ist vor allem deshalb als negativ zu bewerten, da dem HRZ das Problem übernommener Campus-Accounts im Bereich E-Mail seit Langem bekannt ist. Üblicherweise wird die Übernahme eines BHT Campus-Accounts durch untypische Anmeldemuster (Absender-IP-Adresse, Geschwindigkeit) zeitnah erkannt. Dies ist vor allem dann der Fall, wenn die Zugangsdaten bei automatisierten Angriffsversuchen zum Einsatz kommen. Die entsprechenden Accounts werden in solchen Fällen sofort gesperrt, die jeweiligen Personen müssen dann persönlich für eine Passwortrücksetzung das HRZ kontaktieren.
Im Falle des vorliegenden Angriffs fand keine Meldung durch die üblichen internen Überwachungssysteme statt, womit der übernommene Account unerkannt blieb. Es ist davon auszugehen, dass hier gezielt durch die Angreifer eine Entdeckung vermieden wurde, bspw. durch die ausschließliche Nutzung des gekaperten Accounts zu den regulären Arbeitszeiten an der Hochschule. Somit gingen die Angreifer „im Rauschen“ unter.
Das Gefährdungspotential von VPN-Einwahlversuchen mit übernommenen Accounts wurde bisher in den Risikobewertungen offensichtlich nicht ausreichend gewürdigt, und muss dringend mehr in den Fokus gerückt werden.

Frühzeitige Erkennung von laufenden internen Angriffen auf Servern
Eine Installation der campusweit lizensierten Antivirus-Lösung von Trend Micro findet zwangsweise nur innerhalb des HRZ statt, aber XXX. Zum Zeitpunkt des Angriffs waren somit nach Analyse von Trend Micro nur XXX % der Systeme im BHT-Netzwerk von (ihrer) Antiviren-Software aktiv überwacht. Meldungen anderer Antivirus-Software, wie Windows Defender, verblieben auf den lokalen Rechnern und waren somit nicht zentral zu bemerken. Dies ermöglichte es den Angreifern, mehrere Tage unentdeckt auf Systemen von Laboren ungestört zu arbeiten. Hier muss auch betont werden, dass das zum Zeitpunkt des Angriffs benutzte Schadsoftware-Portfolio bereits in den Antivirus-Signaturen bekannt ist. Es wäre somit möglich gewesen, die Scan- und Verschlüsselungsversuche frühzeitig zu erkennen und zu stoppen, bevor die Angreifer sich weiter im Netzwerk bewegen.

Frühzeitige Erkennung von laufenden internen Angriffen im Netzwerk
Die im Verlauf des Angriffs durchgeführten Brute Force – Angriffe auf RDP-Zugänge, sowie der Scan von Netzwerkfreigaben, wurde durch das HRZ nicht erkannt. Der Grund hierfür ist XXX. Somit konnten die Angreifer auch hier ungestört agieren.

Protokollierung von sicherheitsrelevanten Ereignissen
Der vollständige zeitliche Ablauf des Angriffs lässt sich nicht endgültig rekonstruieren, da die Protokolldateien der VPN-Einwahl von der Verschlüsselung betroffen waren und – im Hinblick auf die einzuhaltenden Löschfristen – nicht Teil des Backups sind. Hier muss eine erneute Prüfung der Löschfristen erfolgen.

Fehlendes Asset Management in Laboren
Einige Rechner, wie zum Beispiel „lab3-pc1“, liefen mit einer veralteten Betriebssystem Version (Windows Server 2008), auf der u.a. die bekannte Sicherheitslücke „XXX“ nicht gepatcht war. Dies ermöglichte es den Angreifern, mindestens diesen Computer zu übernehmen. Aufgrund der fehlenden Integration von Labor-Systemen in das zentrale Asset-Management des HRZ werden derartige Software-Stände momentan zentral nicht erkannt.

Isolation von Netzsegmenten
Die Netzwerkinfrastruktur der Labore war bisher nicht ausreichend isoliert, was es Angreifern ermöglichte, zwischen mehreren Laboren und deren IT-Systemen ungestört zu navigieren (*lateral movement*). Verschiedene RDP-Freigaben für Labore existierten hauptsächlich noch als Altlast von Sofortmaßnahmen in der Corona-Krise, und hätten zeitlich begrenzt werden müssen. Teilweise wurden hier vom HRZ, auf Druck der Lehrkräfte, auch potentiell unsichere Freigaben zugelassen.

Kommunikation mit Behörden

Die Sicherheitswarnung der Behörden war zu unspezifisch, um als Auslöser für eine Beauftragung von externen forensischen Unternehmen zu dienen.

Wo hatten wir Glück?

Kein größerer Datenabfluss, kein größerer Datenverlust
Basierend auf den analysierten forensischen Indizien, den auf den Windows-Servern vorgefundenen Artefakten und den vom Deutschen Forschungsnetz bereitgestellten Datenflussprotokollen wird aktuell davon ausgegangen, dass Datenexfiltration stattfand.
Ein signifikanter Datenverlust durch die Verschlüsselung liegt bei den vom HRZ betreuten Systemen nach aktuellem Kenntnisstand nicht vor, da die Sicherungen der zentralen Server und Laufwerke vom Angriff nicht betroffen waren.

Begrenzter Missbrauch eines administrativen HRZ-Account
Die Angreifer nutzen „account3“ ausschließlich für den Zugriff auf den Virtualisierungscluster, und nicht für den Zugriff auf Dateiserver zur Rechteänderung in den Dateifreigaben. Theoretisch wäre dies möglich gewesen.

Angriff ausschließlich auf Windows-Server
Die Angreifer konzentrierten sich ausschließlich auf Windows-Systeme, womit die größtenteils mit Linux realisierten zentralen Systeme (Mail, Moodle, ...) wieder zügig in Betrieb gesetzt werden konnten.

Maßnahmen

HRZ und Präsidium haben in enger Abstimmung verschiedenste Maßnahmen beschlossen, um die von Akira ausgenutzten Sicherheitslücken zu beheben. Dies ist die Grundvoraussetzung, um wieder in einen regulären IT-Betrieb übergehen zu können.

Maßnahme	verantwortlich	Status
Umstellung des VPN-Betriebs auf Mehrfaktorauthentifizierung, um das Eindringen mit gestohlenen Passwörtern von Campus-Accounts zu verhindern.	HRZ	Erledigt, Rollout in Planung.
Sicherheitsscan aller Systeme im Hochschulnetzwerk, um weitere potenziell infizierte Rechner zu identifizieren. Umsetzung eines Ampelsystems zur Kennzeichnung und Wiederinbetriebnahme der Rechner.	HRZ, Multiplikatoren in Laboren	In Arbeit, für HRZ-Systeme und Kernverwaltung abgeschlossen.
XXX	HRZ	Erledigt.
Schutz von lokalen Administrator-Konten auf Computern in der Windows-Domäne der Hochschule mit Microsoft LAPS.	HRZ	Erledigt.
Härtung von Servern und Accounts durch härtere Regularien zum Betrieb von IT außerhalb des HRZ. Dies schließt vor allem die Installation von Antivirus-Software auf Laborsystemen ein.	HRZ, Labore	In Arbeit, Konzept wird erstellt, bis dahin starke Einschränkung der Labornetze.
Zentralisierte Alarmierung bei Antivirus-Meldungen auf Computern, welche mit Trend Micro – Clients ausgestattet sind.	HRZ	Erledigt.
Rücksetzung aller Passwörter in der Windows-Domäne der BHT.	HRZ	Erledigt.
Wiederherstellung aller IT-Dienste nach Abschluss der Sicherungsmaßnahmen.	HRZ	In Arbeit.

Referenzen

[TMIRT] XXX, Trend Micro Incident Response Team Europe, Engagement Report - Berliner Hochschule für Technik, 15.3.2024

Anhang 1 - Begriffe

Begriff	Erläuterung
Hochschulrechenzentrum (HRZ)	Das HRZ betreut als Zentraleinrichtung im Sinne des Berliner Hochschulgesetzes alle IT-Dienstleistungen, die für die gesamte BHT zur Verfügung stehen. Beispiele hierfür sind LAN, WLAN, Anmeldedienste, E-Mail, Speicherdienste, Server-Virtualisierung, Software-Lizensierung, Drucken und zentrale Fachanwendungen. Parallel ist das HRZ für den Betrieb aller Arbeitsplätze der Verwaltungseinheiten der BHT, bspw. Personalabteilung, zuständig.
Labor	Labore sind eigenständige Organisationseinheiten der BHT, welche in vielen Fällen Server und IT-Arbeitsplätze autark beschaffen und betreiben. Die zentralen IT-Dienstleistungen des HRZ (Netzwerk, Anmeldedienste, Speicherdienste, virtuelle Maschinen, Firewall, ...) werden unterschiedlich stark genutzt, häufig liegen historisch gewachsene Strukturen vor. Der Fokus im Betrieb liegt auf der Erfüllung spezieller IT-Anforderungen in Forschung und Lehre, die durch das HRZ als Zentraleinrichtung nicht abbildbar sind.
Campus-Account	Das HRZ betreibt eine zentrale Windows-Domäne, welche für alle Hochschulangehörigen einen Account bietet. Dieser ermöglicht den Zugang zu Mail-Postfächern, dem eigenen Home-Laufwerk, WLAN und anderen zentralen Diensten des HRZ. Das HRZ verwaltet zu jedem Zeitpunkt ca. 18.000 aktive Campus-Accounts für Studierende und Nicht-Studierende.
Active Directory (AD)	Die Windows-Domäne der Hochschule basiert auf einer zentralen Datenbank aller Campus-Accounts, welche als „Active Directory“ bezeichnet wird. Diese enthält die Nutzernamen, verschlüsselten Passwörter und Berechtigungen für alle Campus-Accounts. Zudem werden alle vom HRZ Arbeitsplatz-Geräte im AD verzeichnet.
Domain Controller	Das HRZ betreibt mehrere Server, welche redundant das Active Directory der Hochschule anbieten. Diese werden als „Domain Controller“ bezeichnet.
Server Message Block (SMB)-Freigabe	Computer können Ordner auf der eigenen Festplatte im Netzwerk für den entfernten Zugriff zur Verfügung stellen. Dabei erfolgt die Authentifizierung durch den Freigabe anbietender Computer. SMB-Freigaben werden vom HRZ für sämtliche zentralen Netzlaufwerke verwendet, aber auch von Laboren häufig für eigene Dateifreigaben eingesetzt. Die Absicherung der Freigabe erfolgt anhand lokaler Accounts, welche nur auf dem Computer gelten, oder anhand von Campus-Accounts.

Remote Desktop Protocol (RDP)-Freigabe	Windows-Computer können eine Fernsteuerung ihres Bildschirms aus dem Netzwerk für authentifizierte Nutzer erlauben. Derartige Freigaben werden für die entfernte Administration von Windows-Servern eingesetzt, aber auch zur Umsetzung von virtualisierten Windows-Arbeitsumgebungen, welche unter dem Begriff „Terminal Server“ bekannt sind.
Backdoor	Eine Software, welche von Angreifern auf gekaperten Computern installiert wird. Die Backdoor wartet auf die Verfügbarkeit einer Internet-Anbindung auf dem kompromittierten Computer, und baut dann eine stehende Verbindung zu Computern der Angreifer im Internet auf, welche als „Command & Control (C&C)“ Server bezeichnet werden. Über diese Hintertür haben die Angreifer dann weiterhin Zugriff auf das interne Netzwerk, selbst wenn der originale Angriffsweg abgeschnitten wurde.
Virtual Private Network (VPN)	Eine VPN ist eine Netzwerkverbindung, die von Außenstehenden nicht einsehbar ist. VPN ermöglicht den Inhabern eines Campus-Accounts, die sich außerhalb des BHT-Netzwerks befinden, einen sicheren Zugriff auf das BHT-Netzwerk. Das Einwählen in das VPN ist vergleichbar mit dem Umstecken des Computer-Netzwerkkabels in das durch VPN zugewiesene Netz.