Switch

dem CERT

Geschichten aus ~~der Gruft~~ mit Darja und Silvio

darja-anna.yurovsky@switch.ch
silvio.oertli@switch.ch

Warum Geschichten?

Switch

- Geschichten werde Emotionen
- Lange versucht sensibilisieren bei Leuten zu wecken mit Päsentationen, mit mässigem Erfolg
- bemerkt, dass unser Ansatz gar nicht das ist wie wir Menschen von Kind auf lernen -> Trudi Gerster
- Wie verbeleibt Wissen nachhaltig
- Warum nicht die Gleichen Prinzipien verwenden, wie Menschen/Kinder lernen
- Und darum wollen wir heute mit euch ein paar Geschichten aus der Incident Response Front erzählen, was kann man auch IT-Sicherheitsvorfällen lernen?

Fallstrick 1: Was ist das Problem?

Switch

Geschichte: Falsche Annahmen

Silvio

Der Code des Vertrauens: Eine Geschichte von Integrität und Sabotage

Das 60-Mann-Unternehmen von Kurt Köhler, der Elektro-Solutions GmbH, war seit vierzig Jahren ein Bollwerk der Zuverlässigkeit.

Kurt, ein Patron alter Schule, verstand sein Geschäft als ein Netzwerk des Vertrauens.

Doch dieses Netz begann, unbemerkt zu reißen.

Es begann nicht mit einem lauten Knall, sondern mit einer Dissonanz in der Dispo.

Maria aus der Administration meldete die ersten Phantom-Termine:

Servicetechniker erschienen bei Kunden, die nichts von einer Buchung wussten, während andere, dringende Termine,

laut System einfach verschoben waren und die Kunden vergebliuch auf die Techniker warteten.

Die Störungen eskalierten schnell zur operativen Krise. Stammkunden drohten mit dem Wechsel bei dem aktuellen Servicelevel.

Zugezogene IT Sachkundige analysierten das Kalendersystems und bestätigten die Manipulation.

Doch die User-IDs gehörten den loyalsten Mitarbeitern – Maria, dem Vertriebsleiter, sogar Kurt selbst. Jeder beteuerte, die Termine nicht angerührt zu haben.

Die Firma wurde von einem digitalen Geist sabotiert.

Kurt suchte fieberhaft nach dem logischen Fehler.

Die Wahrheit kam schlussendlich aber nicht aus dem System,

sondern aus einem Gespräch unter vier Augen mit einem Branchenkollegen, Erich.

„Hast du jemandem gekündigt, der Zugriff auf Deine Passwörter hatte?“ fragte Erich.

Die Frage traf Kurt wie ein Schock.

Markus, der kurz zuvor entlassene IT-Administrator. Ein fähiger Mann, aber ohne schon während der Anstellung mit fehlender Loyalität.

In einem Moment geistiger Erschöpfung dämmerte es Kurt: Die Schwachstelle lag nicht im System, sondern auf seinem Schreibtisch.

Kurt erinnerte sich an die ALL_ACCESS.xlsx, seine private, unverschlüsselte Excel-Liste mit allen Master-Passwörtern,

die er in naiver Bequemlichkeit auf seinem Desktop gespeichert hatte.

Markus muss in seinen letzten Wochen, noch mit vollem Systemzugriff, eine digitale Kopie dieser Datei gezogen haben.

Die gestohlenen Credentials waren nun die Waffe. Markus konnte sich, dank fehlender Multi-Faktor-Authentifizierung (MFA), mit Kurts User-ID anmelden und gezielt Termine manipulieren, um die Firma von innen zu zerstören.

Kurt handelte mit der Entschlossenheit eines erfahrenen Handwerksmeisters.

Er ignorierte die Wut und richtete den Fokus auf das Beheben.

In einer Nachtschicht mit externen IT-Beratern wurde sämtliche Passwörter geändert.

Von der kleinsten E-Mail-Adresse bis zum CRM-Master-Zugang, wurden geändert und auf höchste Komplexität gehoben.

Die ALL_ACCESS.xlsx wurde gelöscht.

Am nächsten Morgen herrschte Stille im System.

Die Service-Termine blieben, wo sie hingehörten. Der Geist war gebannt.

Fallstrick 1: Was ist das Problem?

Switch

Geschichte: Cyberpopulismus

Darja

Der Köder des Journalisten: Eine Geschichte von CISO, Phishing und Darknet-Täuschung

Claudio lebte für die digitale Reinheit.

Als CISO eines mittelständischen Technologieunternehmens war seine Passion die Abwehr des Unbekannten,

das ständige Härten der Perimeter. Er fühlte sich als Wächter in einer gut befestigten Festung.

Eines Dienstagmorgens jedoch durchdrang ein Anruf seine professionelle Gelassenheit.

Am anderen Ende der Leitung war Herr Vogel, ein investigativer Journalist mit einer unheilvollen Frage:

„Herr Rossi, was ist Ihre Stellungnahme zu den exfiltrierten Unternehmensdaten,

die eine bekannte Ransomware-Gruppierung über Sie im Darknet zur Verfügung gestellt hat?“

Der Schock war existenziell. Eine Ransomware-Gruppierung? In seinem Netzwerk?

Claudio hatte keinen Payload-Alarm gesehen, keine Verschlüsselung bemerkt, kein Lösegeldforderung auf dem Bildschirm.

Die Stille im System war das Beunruhigendste.

Die Panik im Management war unmittelbar und laut.

Die vom Journalisten genannten Daten stammten aus einem System, das von einem externen Dienstleister

– der Drittfirma SysGuard – betreut wurde.

Die Schlussfolgerung war reflexartig: SysGuard war schuld. Sie hatten das System nicht gehärtet,

sie hatten das Datenleck verursacht. Die Wut wurde zur juristischen Anschuldigung.

Claudio musste handeln. Er bestellte sofort ein Team von Incident Respondern ein, die wie digitale Archäologen begannen,

das vermeintlich betroffene System zu durchkämmen.

Die Responder, angeführt von der kühlen Lena Weber, tauchten tief in die Logs und gleichzeitig das Darknet ein.

Nach Stunden der forensischen Analyse schickte Weber eine knappe Nachricht an Claudio:

"Das Bild stimmt nicht. Nur ein Teil der Daten wurde exfiltriert.

Und zwar nicht aus dem SysGuard-System. Auch fehlen auf den Systemen hinweise auf die Ransomware Gruppierung komplett."

Claudio, nun nicht mehr panisch, sondern von kalter Entschlossenheit getrieben,

forderte die vollständige Rekonstruktion des Angriffsvektors.

Die Analyse führte die Responder auf eine allzu übliche Spur.

Und mussten feststellen, dass zwei Mitarbeiter aus unkritischen Abteilungen auf eine hochprofessionelle Phishing-Kampagne hereingefallen waren.

Sie hatten ihre Credentials auf einer gefälschten Anmeldeseite eingegeben.

Dabei war die Gruppe, die die Daten tatsächlich gestohlen hatte, keine Ransomware-Gruppierung,

sondern eine auf Datendiebstahl spezialisierte Organisation, die gestohlene Informationen sammelte.

Die berühmte Ransomware-Gruppierung hatte die Daten nicht selbst gestohlen.

Sie hatte lediglich den Link zur Datensammlung der anderen Gruppe im Darknet publiziert.

Es war ein Akt der medialen Aggression – sie nutzten ihren berüchtigten Namen und die

Angst,

um Aufmerksamkeit für das Leck zu generieren, das sie gar nicht selbst verursacht hatten.

SysGuard war unschuldig.

Claudio, der CISO, sah die Ironie:

Die größte Bedrohung für seine Festung war nicht ein komplizierter Zero-Day-Exploit,

sondern der Klickfehler zweier Mitarbeiter.

Die Anschuldigungen des Vorstands waren falsch, die Berichterstattung des Journalisten

manipuliert durch einen Cyber-Marketing-Trick der Angreifer.

Claudio musste nun nicht nur das Leck schließen, sondern vor allem die Wahrheit im Management verankern:

Im Krieg um Daten ist nicht immer der lauteste Name der wahre Feind –

und Awareness ist der wichtigste Patch, den man installieren kann.

Fallstrick 2: Risk Assessment

Switch

Geschichte: Wir dachten wir sind vorbereitet

Silvio

Die Rückkehr der Bänder: Eine Geschichte von Hubert und der unterschätzten Wiederherstellung

Hubert war die gute Fee der Maschinen. Seit Jahren sorgte der Systemadministrator dafür,

dass die digitalen Zahnräder der mittelständischen Fabrik geschmiert liefen.

Er kannte jeden Server mit Namen und wusste um deren Schwachstellen.

Eine seiner grossen Leistung war die Backup-Strategie. Sie schien makellos: Alle kritischen Systeme wurden täglich auf physische LTO-Tapes gesichert,

sicher verwahrt in einem feuerfesten Safe. Das Risiko-Assessment hatte das Feld "Backup vorhanden" mit einem beruhigenden "Grün" markiert.

Eines Montagmorgens, als Hubert seine Konsole hochfuhr, schlug die Realität mit brutaler Wucht zu.

Rote, verschlüsselte Warnmeldungen blinkten auf fast jedem Bildschirm.

Ein Ransomware-Exploit, der sich in der Nacht lautlos ausgebreitet hatte, hatte die gesamte Produktions- und

Verwaltungsinfrastruktur lahmgelegt. Der Albtraum eines jeden ITlers war eingetreten.

Panik breitete sich in den Büros aus.

Der Geschäftsführer stürmte zu Hubert: "Wir haben doch Backups, Hubert! Wie lange dauert es?"

Hubert blieb ruhig, wissend um die Tapes im Safe. "Wir haben Backups, Herr Direktor. Die Daten sind sicher."

Er holte die neuesten Bänder.

Doch als Hubert die Wiederherstellung starten wollte, entfaltete sich der wahre Schrecken des unvollständigen

Risk Assessments.

Das Unternehmen verfügte nur über ein einziges funktionierendes, modernes Bandlaufwerk.

Die moderne IT-Architektur, konzipiert für Effizienz im Regelbetrieb, war zur Engpass-Katastrophe geworden,

als die Krise eintrat.

Hubert rechnete kurz im Kopf durch: 20 Server, Terabytes an Daten.

"Mit diesem einen Laufwerk, unter Volllast, mit dem Wechsel der Bänder... würde die vollständige Wiederherstellung

des Betriebs drei bis vier Wochen dauern," musste Hubert dem entsetzten Management berichten.

Vier Wochen Stillstand bedeutete den wirtschaftlichen Tod der Firma.

Der grüne Haken im Risk Assessment war eine gefährliche Illusion geworden.

Hubert, der sich weigerte, aufzugeben, wusste, dass die Antwort nicht in der teuren Neubeschaffung lag (die Wochen dauern würde),

sondern im Netzwerk der Beziehungen.

Er erinnerte sich an den die Gruppe von Systemadministraoren, die sich monatlich zu einem Stammtisch trifft. Er zèckt sein telefon und nach ein paar Anrufen, kann er fèr einige Tage Laufwerke von anderen Administraotoren ausleihen.

Hubert zog die Laufwerke triumphierend ans Licht. Baute mit den Laufwerken und einigen Servern eine regelrechte Recoveryfarm auf.

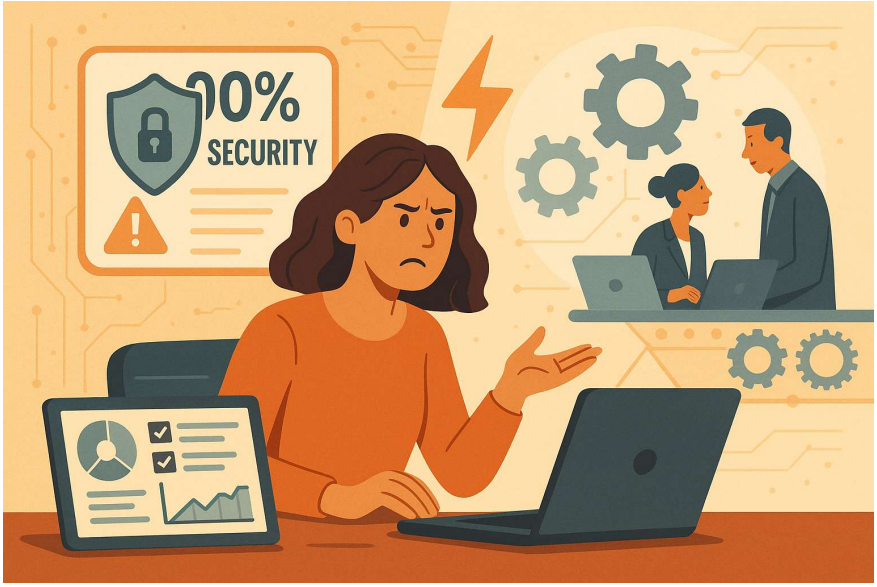
Der Geschäftsführer sah nicht nur die gerettete Firma,

sondern verstand die wahre Lektion: Ein Risiko ist erst dann beherrschbar,

wenn man nicht nur die Backup-Strategie, sondern auch die Recovery-Strategie – inklusive der notwendigen Hardware-Redundanz – vollumfänglich testet und bewertet.

Hubert, der gewissenhafte Administrator, hatte nicht nur die Daten gerettet;
er hatte die Wahrheit über die Wiederherstellung ans Licht gebracht,
indem er sein persönliches Netzwerk aktivierte.

Fallstrick 2: Risk Assessment



Switch

Geschichte: Spannungsfeld zwischen Perfekter Sicherheit und Realität

Darja

Die Null-Toleranz-Illusion: Eine Geschichte von Kai und der Wertschöpfungskette

Kai war frisch gebackener IT Spezialist. Seine Masterarbeit in Cyber-Abwehr hatte eine theoretisch unknackbare Architektur entworfen.

Für ihn gab es nur einen Zustand: 100 Prozent Sicherheit. Alles andere war fahrlässig.

Als er seine erste Stelle als Junior Security Analyst bei einem großen Logistikunternehmen antrat,

sah er das Netzwerk als eine Ansammlung von Schwachstellen, die nur auf ihren Patch warteten.

Sein erster großer Konflikt war das Legacy-Versandterminal – ein uralter Rechner,

der die automatische Beladung von Containerschiffen steuerte.

Kai stellte fest: Das Betriebssystem war End-of-Life, die Firmware ungepatcht, die Konfiguration ein Albtraum.

Ein Hochrisiko-System.

Kai marschierte zu seinem Vorgesetzten, dem CISO, mit dem Ausdruck eines Kreuzzüglers.

„Dieses Terminal muss sofort abgeschaltet werden, oder zumindest vom Netz isoliert!

Es ist ein Tor für jeden Angreifer. Wir müssen Bulletproof sein.“

Der CISO lächelte müde. „Kai, Ihre Analyse ist technisch korrekt.

Aber dieses Terminal steuert das Beladen von fünf Schiffen pro Tag.

Fünf Stunden Ausfall kosten uns eine halbe Million Euro. Das nennen wir Wertschöpfung.

Wir können nicht einfach abschalten."

Kai verstand nicht. In der Uni war Sicherheit das höchste Gut.

Im Unternehmen schien Geschäftskontinuität das höchste Gut zu sein.

Die Lektion kam, wie so oft, in Form eines Incidents.

Ein unvorsichtiger Mitarbeiter öffnete eine scheinbar harmlose PDF,

die sich als Advanced Persistent Threat (APT) entpuppte. Der Schädling breitete sich schnell aus und begann,

kritische Konfigurationsdateien zu manipulieren.

Kai war als Teil des Incident Response Teams im Einsatz.

Seine erste Reaktion: Alles trennen! Er schlug vor, sofort das gesamte Netzwerk herunterzufahren,

um eine Ausbreitung zu verhindern – der "Total Isolation"-Ansatz aus dem Lehrbuch.

Doch der Incident Manager stoppte ihn. „Kai, wir müssen Containment betreiben, nicht Zerstörung.

Wenn wir jetzt das gesamte Logistiksystem kappen, stehen weltweit 500 Lkw still und

Waren im Wert von 10 Millionen Euro werden nicht ausgeladen. Wir müssen einen chirurgischen Eingriff vornehmen."

Kai verbrachte die nächsten 36 Stunden im Spannungsfeld der Enterprise Security.

Er lernte, dass jede Entscheidung eine Risikoabwägung war:

- Risiko A: Das System sofort offline nehmen und hohe finanzielle Verluste in Kauf nehmen (100 % Sicherheit, 0 % Wertschöpfung).

- Risiko B: Den Angriff beobachten, die Ausbreitungsgeschwindigkeit gegen die Wiederherstellungszeit abwägen

und nur die am stärksten kompromittierten Segmente isolieren,

um die Kern-Wertschöpfungskette (Warenauslieferung) am Leben zu halten.

Er musste nicht nur den digitalen Feind verstehen, sondern auch mit der Produktionsleitung kommunizieren,

die keine IT-Sprache sprach, aber die genauen Auswirkungen jedes abgeschalteten Servers auf die Lieferkette kannte.

Es war ein zutiefst interdisziplinärer Job.

Am Ende gelang es dem Team, den Angreifer zu isolieren, ohne die kritischsten Geschäftsprozesse lahmzulegen.

Der Schaden war begrenzt, die Wertschöpfungskette gehalten.

Kai verließ den Krisenraum nicht als der Idealist, der an 100 Prozent Sicherheit glaubte.

Er verstand nun: Enterprise Security ist kein Kampf um ein Bulletproof System.

Es ist eine Balance – ein ständiges Abwägen von Risiko gegen den wirtschaftlichen Nutzen,

eine Aufgabe, die hohe Kommunikationsfähigkeit erfordert, um mit dem Rest des Unternehmens im Einklang zu bleiben.

Seine neue Mission war nicht mehr die Eliminierung aller Risiken,

sondern die effiziente Beherrschung der Risiken im Dienste der Geschäftskontinuität.

Fallstrick 3: Sicherheit ist interdisziplinär

Switch

Geschichte: der IT Vorfall trifft auf den Krisenstab

Silvio

Die Silo-Sprengung: Eine Geschichte von Clara und dem interdisziplinären Notruf

Clara war eine erfahrene Security Analystin im Kernteam eines mittelständischen Dienstleisters.

Sie sah das Unternehmen als ein komplexes, aber beherrschbares System.

Ihre Welt waren Logs, Metriken und technische Protokolle.

Eines Mittwochnachmittags leuchtete das Dashboard mit höchster Dringlichkeit auf.

Eine Zero-Day-Schwachstelle in einem weit verbreiteten Service war aktiv ausgenutzt worden.

Das war kein Phishing-Angriff, den man mit Schulungen beheben konnte; das war ein direkter Einbruch

in die Infrastruktur.

Clara handelte nach dem Buch: Sie containte das Leck sofort und erstellte einen technischen Bericht

über die Ausbreitung und die notwendigen Korrekturen. Dann ging sie zum Geschäftsführer, Herrn Lehmann.

"Herr Lehmann, wir haben einen ernsten Einbruch.

Wir müssen sofort einen Krisenstab einrichten, die Kunden informieren und

die Rechtssicherheit prüfen lassen," erklärte sie sachlich, den technischen Bericht in der Hand.

Herr Lehmann, dessen Fokus auf der aktuellen Akquise lag, winkte ab.

"Frau Wagner, ich vertraue Ihnen und der IT.

Machen Sie es einfach wieder heil. Das ist eine technische Sache,

keine Krise des Unternehmens."

Zurück an ihrem Schreibtisch wurde Clara von Stakeholdern bombardiert.

Der Vertriebsleiter forderte sofort Auskunft, welche Kundendaten betroffen waren – er musste verkaufen.

Die Rechtsabteilung wollte wissen, ob die DSGVO verletzt wurde – sie wollte klagen.

Der Controller wollte eine genaue Kostenschätzung – er wollte sparen.

Clara, fixiert auf die Eliminierung des Schädlings, wollte von den nicht-technischen Fragen nichts wissen,

die im Minutentakt auf sie einprasselten. Sie war allein in der technischen Kommandozentrale,

aber das Chaos tobte in der organisatorischen Leere um sie herum.

Der Geschäftsführer sah sich nicht in der Verantwortung; die Krise blieb im IT-Silo gefangen.

Völlig entmutigt machte Clara eine kurze Pause an der Kaffeemaschine.

Dort traf sie Jenny, die Kommunikationsleiterin. Jenny war eine energetische Person,

die normalerweise nur bei echten (physischen) Notfällen wie Feuer oder

Unfällen in den zentralen Krisenstab berufen wurde.

"Du siehst aus, als hättest du gegen eine Firewall gekämpft," bemerkte Jenny.

Clara seufzte und erzählte kurz von der technischen Invasion und ihrer Frustration über die Stakeholder-Anfragen.

Jenny wurde schlagartig ernst. "Moment mal. Wenn du gehackt wurdest,

Kunden betroffen sein könnten und die Rechtsabteilung Fragen hat... das ist kein IT-Problem.

Das ist eine Unternehmenskrise."

Jenny bot ihre Hilfe an. Sie erkannte, dass die IT-Sicherheit zwar die technische

Lösungsstrategie lieferte,

aber der Prozess der Krisenbewältigung in jedem Unternehmen derselbe ist.

Innerhalb einer Stunde hatte Jenny, mit der Autorität ihres üblichen Krisenstabspostens,

den gesamten klassischen Krisenstab einberufen – bestehend aus HR, Recht, Kommunikation und

Geschäftsleitung (die nun doch erschien).

Der Stab erkannte schnell, dass Claras technischer Vorfall alle Facetten einer echten Katastrophe hatte:

- Kommunikation (Jenny) musste die Kunden und Medien beruhigen.
- Recht musste die Einhaltung der Vorschriften sicherstellen und Klagen abwehren.
- HR musste die Mitarbeiter informieren.

Clara lieferte die Fakten und die technische Lösungsstrategie (Wiederherstellung, Patching).

Doch erst durch die interdisziplinäre Operation des Krisenstabs wurde aus der technischen Behebung

eine organisatorisch beherrschte Krise.

Für Clara war es die größte Lektion: Ein IT-Sicherheitsvorfall ist nur am Anfang ein technisches Problem.

Im Enterprise-Umfeld ist es eine interdisziplinäre Operation, die eine hohe Kommunikationsfähigkeit erfordert,

um die gesamte Organisation aus ihrem Silo zu holen und die Krise gemeinsam zu bewältigen.

Die Wahrheit liegt nicht nur in den Logs, sondern in der gemeinsamen Reaktion.

Fallstrick 4: Digitale Interdependenz

Switch

Geschichte: E-Mails laufen wieder – aber keiner kommt rein

Darja

Die Logik der Tür: Eine Geschichte von Peter und der physischen Abhängigkeit

Peter Schneider, CEO eines mittelständischen Softwareentwicklungsunternehmens,

war stolz auf seine Hybrid-Infrastruktur. Die wichtigsten Applikationen liefen zwar in der Cloud,

doch die heiligen Kerne – Dateiserver, das Mailsystem und die zentrale Datenbank –

lagen sicher im eigenen, kleinen Data Center im Keller des Hauptgebäudes.

Eines Dienstagmorgens fand Peter Schneider nicht die übliche Produktivität,

sondern eine digitale Stille. Ein flächendeckender Ransomware-Angriff hatte die gesamte

On-Premise-Infrastruktur lahmgelegt und die Dateien verschlüsselt.

Peter, der als CEO die oberste Verantwortung trug, musste nun die Prioritäten für die Wiederherstellung festlegen.

Er berief das kleine, überforderte IT-Team zusammen.

"Wir brauchen Kommunikation!" befahl Peter. "Der Markt muss wissen, dass wir handlungsfähig sind,

die Kunden müssen beruhigt werden. Wir starten mit dem Mailsystem."

Die IT-Mitarbeiter zogen sich in das kühle, schallisolierte Data Center zurück,

um die Recovery-Prozesse einzuleiten. Die erste Aufgabe: die Wiederherstellung des Exchange-Servers aus den Backups.

Peter, selbst in der Hektik des Geschehens, versuchte, die Moral zu halten,

Anrufe entgegenzunehmen und mit Partnern zu sprechen.

Nach drei Stunden intensiver Arbeit spürte er die Anspannung.

Er beschloss, in die Cafeteria zu gehen, um sich einen Kaffee zu holen und kurz durchzuatmen.

Er steckte seine elektronische Zugangskarte in das Lesegerät seines Büros.

Ein Piepen. Rot. Die Tür blieb verschlossen.

Verwirrt versuchte er es an der Tür des Sekretariats. Auch hier: Rot. Kein Zugang.

Ihm fiel ein, als würde ein digitales Dominospiel im Nachhinein zusammenbrechen:

Das gesamte elektronische Schließsystem des Gebäudes, das die Zugänge zu Büros, Laboren

und vor allem zum Data Center regelte, war auf einem der wenigen lokalen Server gehostet.

Und dieser Server war, wie alle anderen, verschlüsselt und offline.

Er klopfte an die Außentür des Rechenzentrums. Sein IT-Mitarbeiter öffnete, blickte irritiert.

"Die Schließanlage ist tot," stellte Peter fest, seine Stimme war plötzlich leiser.

"Wenn ihr jetzt in die Pause geht oder die Schicht wechselt... kommt ihr nicht wieder rein."

Der Schock wich der kalten, harten Logik der Wertschöpfungskette.

Wenn die elektronischen Zugangskarten nicht mehr funktionierten, konnten die IT-Mitarbeiter

nach dem Schichtwechsel nicht mehr ins Gebäude, geschweige denn in das Data Center, um die

Recovery-Arbeiten fortzusetzen. Auch wenn das Mailsystem wieder lief:

Die manuelle Arbeit zur Wiederherstellung der Systeme wäre physisch blockiert.

Peter traf eine neue, harte Entscheidung, die direkt der physischen Betriebskontinuität diente:

Stop: Sofortiger Stopp der E-Mail-Wiederherstellung.

Redirect: Umleitung aller IT-Ressourcen zur sofortigen Wiederherstellung des Schließsystem-Servers.

Die Recovery-Priorität hatte sich abrupt vom immateriellen Gut (Kommunikation) auf das physische Gut (Gebäudezugang) verschoben.

Die IT-Mitarbeiter arbeiteten unter Hochdruck, um den Schließsystem-Server wiederherzustellen.

Erst als das Zugangsmanagement wieder grün zeigte und die elektronischen Karten funktionierten,

war die Kette der Wiederherstellung gesichert.

Peter hatte an diesem Tag die tiefere Lektion über Incident Response gelernt:

In einem KMU ist die digitale Verfügbarkeit untrennbar mit der physischen Verfügbarkeit verbunden.

Die kritischsten Systeme sind nicht immer die offensichtlichsten; manchmal ist das wichtigste System das,

das die Tür öffnet, damit die Arbeit überhaupt erst erledigt werden kann.

Fallstrick 4: Digitale Interdependenz

Switch

Geschichte: Was ist wirklich kritisch?

Silvio

Das Paradoxon der Pille: Dr. Melanie Fischer und die Stille im Spital

Das St.-Vincent-Klinikum galt als digitale Speerspitze der Gesundheitsversorgung.

Die Digitalisierung war so tief integriert, dass selbst die Essensbestellung der Patienten über eine App lief.

Dr. Melanie Fischer, Onkologin und Verfechterin des digitalen Wandels,

war stolz auf die Effizienz ihres Arbeitsplatzes.

Doch eines Montagmorgens war die Effizienz ausgelöscht.

Auf dem Monitor des MRT (Magnetresonanztomographen) erschien eine rote, unheilvolle Botschaft:

eine Ransomware-Forderung. Das war nicht der Anfang des Problems, das war nur der öffentliche Beweis.

Das Spital reagierte blitzschnell und nach Protokoll: Hard-Isolation. Das gesamte Netzwerk wurde vom Netz genommen.

Innerhalb weniger Stunden kehrte das Spital in die analoge Steinzeit zurück.

Melanies Team musste Visiten wieder mit dicken, unhandlichen Papierakten durchführen,

deren Seiten vergilbt und unvollständig schienen. Die Patienten wählten ihr Mittagsmenü wieder auf kleinen Zetteln.

Die Versorgung war gewährleistet, aber die Fehlerrate und der Stresslevel stiegen exponentiell.

Nach einer Woche im Offline-Notbetrieb war der Chief Information Security Officer (CISO)

mit der schwersten Entscheidung konfrontiert: Welche Systeme werden zuerst hochgefahren?

Die Recovery-Priorität musste festgelegt werden.

Melanie saß im Krisenstab, um die Sicht der Ärzte zu vertreten. Ihre Forderung war klar und lebenswichtig:

"Die medizinischen Kerngeräte müssen zuerst laufen! Der Linearbeschleuniger für die Bestrahlung,

die Überwachungssysteme auf der Intensivstation und die Notfallaufnahme.

Das SAP-System? Das kann warten. Ob wir unsere Stunden jetzt aufschreiben oder in einer Woche –

wen interessiert das im Angesicht der Patientensicherheit?"

Der CISO stimmte der klinischen Priorität grundsätzlich zu.

Doch ein ruhiger Mitarbeiter aus der Logistik meldete sich zu Wort.

"Herr CISO, Dr. Fischer hat recht. Die Patientenversorgung ist das Wichtigste.

Aber es gibt ein Problem mit dem SAP."

Es stellte sich heraus, dass das SAP-Modul nicht nur für die Abrechnung und die Lohnbuchhaltung zuständig war

– die als "unwichtig" galten. Das Spital hatte die Lagerverwaltung und die automatische Nachschubsteuerung

aller Verbrauchsmaterialien und Medikamente tief in das Enterprise Resource Planning (ERP), sprich,

das SAP, integriert.

Der Mitarbeiter erklärte: "Wir haben noch Vorräte für 12 Stunden.

Aber die Automatisierung der Apotheke, die Bestellung der Spezial-Chemotherapeutika und

der tägliche Nachschub an gängigen Schmerzmitteln – alles läuft über die Bestell-Schnittstelle des SAP.

Wenn wir das System nicht hochfahren, um Nachschub zu bestellen,

haben wir bald zwar funktionierende Bestrahlungsgeräte, aber keine Betäubungsmittel mehr."

Dr. Fischer erkannte mit Schrecken das Paradoxon der Pille.

Die medizinischen Geräte waren nutzlos, wenn die logistische Kette brach.

Das unscheinbare SAP, das System der Buchhaltung, war in Wahrheit der Schlüssel zur Patientenversorgung.

Die Priorität musste sich ändern: Die Wiederherstellung des SAP-Kernmoduls zur

Sicherstellung des Medikamentennachschubs musste vor vielen klinischen Systemen erfolgen,

um die Gesamtversorgung längerfristig zu gewährleisten.

Melanie verstand: IT-Sicherheit und Recovery im Gesundheitswesen sind keine rein technischen Entscheidungen,

sondern eine Kette von Abhängigkeiten. Die wahre Priorität liegt dort,

wo die unterstützende Logistik auf die klinische Behandlung trifft.

Die Gefahr lauert nicht nur im Virus, sondern in der Unkenntnis der systemischen Abhängigkeiten.

Fallstrick 5: Beschämen vs. Befähigen

Switch

- Aus Sicht von Awareness Spezialist: Phishing-Tests (wir Wissen schon lange, dass diese Tests nichts bringen, es gibt wissenschaftliche Studien dafür und trotzdem machen es alle für den Management Check). IT Consulting Firmen, die Menschen immer noch Angst machen und die Grundprinzipien der Pädagogik nicht begriffen bzw. Verstehen nicht dass der Effekt nur kurzfristige Bewältigungstrategien hervorruft, aber hält harnäckig im Feld

Fallstrick 5: Beschämen vs. Befähigen

Switch

Geschichte: Gemeinsam Gegen die Risiken

Lena

Der Kodex der Erzählung: Eine Geschichte von Lena und dem Ende der Angst

Lena Weiss war Awareness-Spezialistin und fühlte sich oft wie eine Missionarin in einem Land der digitalen Mythen.

Sie kämpfte gegen die hartnäckigsten Überzeugungen der IT-Branche: Angst führt zu Sicherheit.

Ihre schlimmste Schlacht war der halbjährliche Phishing-Test.

Die Ergebnisse wurden dem Management präsentiert, der "Versagensquote" eine Zahl zugeordnet und

die "Gefallenen" – die Mitarbeiter, die geklickt hatten – wurden in Mails verpackt, die subtil

zwischen Shaming und Belehrung schwankten. Wissenschaftliche Studien zeigten Lena schon lange,

dass diese Taktik nutzlos war; sie bewirkte nur kurzfristige Bewältigungsstrategien und eine

generelle Abneigung gegen alles, was mit "Security" zu tun hatte.

Lenas Vorgesetzte, die IT-Beratungsfirmen, propagierten weiterhin die Angst.

Sie lieferten dem Management die einfache Checkbox-Lösung: Test bestanden? Risiko gering.

Test nicht bestanden? Weiter Angst schüren. Die Grundprinzipien der Pädagogik –

Empathie,

positives Lernen, das Vermeiden von Negativverstärkung – wurden für einen schnellen, aber

oberflächlichen Effekt geopfert.

Doch Lena hatte eine neue Vision. Sie wollte die Geschichten des Unternehmens nutzen –

die Geschichten von Patron Kurt, der beinahe durch gestohlene Passwörter zugrunde ging;

von CISO Claudio, dessen Team beinahe eine unschuldige Drittfirma beschuldigte; von Admin Hubert,

der in der Krise auf alte, vergessene Ressourcen zurückgreifen musste;

von CEO Peter, der lernte, dass die Tür wichtiger ist als die E-Mail.

Lena entwickelte ein Konzept: das "Collaborative Security Storytelling".

Die Idee war, die War Stories nicht als Beispiele des Versagens, sondern als Fallstudien

gemeinsamer Herausforderungen in die Schulungen zu integrieren.

Sie holte sich die IT-Experten (Claudio, Hubert und Kai) mit ins Boot.

Anstatt passiv zuzuhören, wurden die Mitarbeiter des Management Boards und

der Fachabteilungen in interdisziplinären Workshops zu Akteuren.

Die Gruppe las die Geschichte von Huberts Backup-Krise.

Dann stellte Lena die Frage, die einem Dungeons & Dragons (D&D)-Szenario glich:

"Okay, Team. Wir haben 48 Stunden. Wir müssen vier Laufwerke anschließen.

Das Logistik-System braucht 12 Stunden. Das HR-System 6 Stunden.

Was sind unsere drei Pre-Approved-Actions, um die Produktion am Laufen zu halten?"

Die Teilnehmer diskutierten nicht über Technik, sondern über Wertschöpfungskette,

Logistik und Kommunikation. Sie mussten ein gemeinsames Verständnis für die vor- und

nachgelagerten Aktionen entwickeln.

Die Sprache änderte sich. Die Mitarbeiter lernten, die IT nicht als Schwarze Kiste,

sondern als Zahnrad zu sehen, dessen Ausfall die eigene Abteilung direkt betraf.

Lena etablierte die "Ja, und..."-Kultur in der Security-Kommunikation.

Anstatt: "Ja, wir könnten das System patchen, aber es könnte abstürzen (Angst/Abwehr).",

sagten sie: "Ja, wir müssen das System patchen, und deshalb arbeiten wir mit der Produktion zusammen,

um einen 30-minütigen Wartungs-Slot zu finden (Zusammenarbeit/Lösung)."

Der Management Check war nicht länger die Phishing-Quote, sondern die messbare Verbesserung

der interdisziplinären Reaktionsfähigkeit.

Lena hatte ihr Ziel erreicht.

Sie hatte bewiesen: Wirklich wirksame IT-Sicherheit wird nicht durch Angst und Scham erzeugt,

sondern durch Empathie, Verständnis und die kollektive Erzählung von Geschichten,

die das gesamte Unternehmen in die Verantwortung nehmen. Die "Techno-Novellen" wurden zum Kodex für eine neue,

kollaborative Sicherheitskultur.

Wer sind wir

Darja-Anna Yurovsky

Co-Head CERT & SOC
Senior Security Engineer
MSc Digital Forensics, MA Data Science
@Switch since 2020
DFIR, LE, Forensic Readiness, Security Advocacy etc.

darja-anna.yurovsky@switch.ch

Silvio Oertli

Co-Head CERT & SOC
Senior Security Engineer
Dipl. Ing. FH tech. Inf., BLaw
@Switch since 2015
Experience in Firefighting, Investigations, IT-Forensics, Programming, Dungeon Mastering, etc.

silvio.oertli@switch.ch

Switch

12

- Hobby: passionierte Geschichtenerzähler:in
- Beruflich: vollblut Incident Responder:in und Weltverbesserer

Woher kommen wir

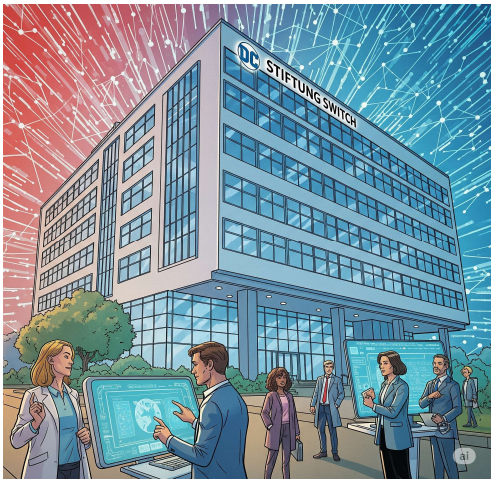
Stiftung der Universitätskantonen und Bund

Gegründet 1987

Non Profit

Internet Service Provider Hochschulen und Forschungseinrichtungen

Registry für .ch/.li



Switch
CERT